+

Marco de Interoperabilidad Técnico

V1.2 - 19 de mayo de 2026

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

V1.2 - 19/05/2026

Contenido

1. Introducción

Durante los últimos años, Europa y España han recorrido un camino decisivo en la construcción de un marco político, regulatorio y técnico para impulsar la economía del dato y habilitar los espacios de datos como instrumentos estratégicos para la competitividad, la innovación y la transformación digital.

Los espacios de datos requieren de una base técnica común que garantice la comunicación, la compatibilidad y la confianza entre múltiples participantes y sistemas heterogéneos. Para asegurar que estas infraestructuras público-privadas digitales operen de forma coherente, segura y alineada con los principios de soberanía del dato, es necesario disponer de un marco técnico que defina los correspondientes mecanismos de interoperabilidad.

El presente documento establece dichos elementos, proporcionando una referencia transversal, práctica y estandarizada para el diseño, despliegue y operación de espacios de datos en cualquier dominio.

1.1. Contexto y justificación

La primera Estrategia Europea de datos situó la economía el dato en el centro de la agenda digital europea, proponiendo la creación de los Common European Data Spaces (CEDS) como infraestructuras federadas para dinamizar sectores estratégicos como salud, movilidad, energía, agricultura o industria. A esta visión se sumaron iniciativas como SIMPL-Open (que proporciona una base tecnológica de middleware interoperable, alineada con estándares europeos de espacios de datos, que puede ser reutilizada para la implementación de los servicios habilitadores descritos en este marco), Data Spaces Support Center (DSSC) proporcionando algunas indicaciones, buenas prácticas, patrones y recomendaciones de alto nivel para la creación de espacios de datos, Comité Europeo de Innovación en materia de Datos (CEID) – creada por la DGA como órgano consultivo europeo para orientar políticas, estándares y prioridades en la economía del dato -, Data Spaces Business Alliance (DSBA) – que agrupa asociaciones europeas y actores industriales para fomentar la armonización de requisitos y modelos de referencia-, etc.

En paralelo, la Unión Europea ha aprobado un marco legal robusto orientado a garantizar la confianza y la equidad en el acceso y uso de datos entre organizaciones: el Data Governance Act (DAG), el Data Act, la legislación asociada a la IA y otras piezas normativas sectoriales. Este marco se complementa con el Reglamento eIDAS2, que introduce la Identidad Digital Europea, reforzando los mecanismos de autenticación, verificación y atribución necesarios para operar de forma confiable en entornos colaborativos como los espacios de datos. En conjunto, estas normas regulan condiciones de acceso, modelos de uso, obligaciones de protección, derechos contractuales y mecanismos para incentivar la reutilización de datos públicos, privados e industriales.

A pesar de la riqueza de iniciativas, avances conceptuales, prototipos y contribuciones técnicas, existe un gap evidente, Europa ha desarrollado una visión firme y un marco regulatorio sólido, pero no existe aún una especificación práctica, clara, adoptable y prescriptiva para construir un espacio de datos funcional e interoperable end-to-end.

La reciente nueva estrategia europea de datos (2024) ha reforzado esta necesidad al vincular los espacios de datos con la IA, los Datalabs y los sandboxes regulatorios, subrayando que la interoperabilidad debe resolverse de forma decidida si se quiere extraer valor real de los datos.

En España, el despliegue del Plan de Impulso de los Espacios de Datos (PIED) ha marcado un punto de inflexión en la construcción de un ecosistema nacional orientado a la creación de valor a partir del dato. El PIED ha articulado inversiones estratégicas, marcos de actuación y proyectos tractores que han generado una demanda creciente de orientación técnica por parte de administraciones, empresas y centros tecnológicos. A ello se suma la publicación de la UNE 0087:2025, las convocatorias financiadas del Plan de Recuperación, los centros demostradores, los casos de uso sectoriales y el trabajo continuado de la SEDIA para consolidar un enfoque común sobre espacios de datos en España.

En este contexto, el Centro de Referencia de Espacios de Datos (CRED) ha asumido un papel central como agente coordinador y generador de conocimiento, impulsando la reciente Hoja de Ruta de Marcos de Referencia y publicando un conjunto de documentos técnicos —incluyendo este Marco de Interoperabilidad Técnico, Guía de Gobernanza de Espacios de Datos, Guía del Promotor, Guía del Participante, Guía de Verificación de Conformidad con la Especificación UNE 0087:2025 (4), y otras guías complementarias disponibles en (https://cred.digital.gob.es/marcos-de-referencia).

Estas iniciativas han acelerado de manera decisiva la conversación nacional sobre interoperabilidad, gobernanza y diseño de espacios de datos. Sin embargo, este impulso también ha puesto de manifiesto una necesidad compartida por todos los actores implicados: disponer de un marco técnico claro, práctico y adoptable, que oriente el diseño y despliegue de espacios de datos interoperables y que garantice que participantes, plataformas y servicios habilitadores puedan operar entre sí, tanto dentro de un espacio de datos como entre distintos ecosistemas sectoriales o territoriales.

La norma UNE 0087:2025 proporciona una caracterización detallada de los espacios de datos y define los principios que guían su interoperabilidad legal, organizativa, semántica y técnica. Este marco desarrolla de manera transversal y desde una perspectiva técnica la implementación de dicha interoperabilidad, proporcionando una referencia unificada para su implantación práctica en espacios de datos.

El propósito principal de la interoperabilidad es conseguir tanto que cada espacio de datos sea capaz de desplegar la arquitectura necesaria para que sus participantes puedan intercambiar datos, como que varios proyectos sean interoperables entre sí, componiendo ecosistemas de intercambio mayores y federados.

La prioridad actual es clara; conseguir que en primer lugar los proyectos alcancen la interoperabilidad entre participantes, logrando el despliegue de sus casos de uso, incorporación de participantes y datos, poniendo el foco en validar su idoneidad, sostenibilidad, retorno e impacto de negocio y mercado.

Por otro lado, conseguir la interoperabilidad entre espacios de datos es un objetivo alcanzable y de gran valor, pero que puede presentarse complejo técnicamente teniendo en cuenta el actual estado del arte. Las iniciativas que necesiten alcanzar la

implementación de la interoperabilidad entre espacios de datos para la consecución de sus casos de uso, objetivos de negocio y retorno, deberán priorizar también este reto.

1.2. Histórico de versiones

Versión	Cambios	Justificación
v.1	Versión Inicial	
	Inclusión de Simpl como tecnología habilitadora	La tecnología Simpl, middleware desarrollado por la Comisión Europea para la construcción de espacios de datos, se incorpora al Marco de Interoperabilidad Técnico como una apuesta estratégica para la futura convergencia e interoperabilidad entre los espacios de datos nacionales y con los europeos.
v. 1.2	Aportaciones recibidas a través del Subcomité 43 - UNE	Mejoras en terminologías y clarificación de conceptos generales.

1.3. Relación con la Estrategia Europea de Datos y la Norma UNE 0087:2025

El presente marco se alinea con los objetivos de la Estrategia Europea de Datos que impulsa la creación de espacios comunes de datos interoperables para sectores como salud, industria, movilidad, energía, finanzas o administración pública. Esta estrategia promueve la compartición de datos bajo principios de soberanía, transparencia, seguridad y accesibilidad.

En particular, este documento se fundamenta en los principios técnicos recogidos en la UNE 0087:2025, que establece las características y capacidades esenciales que deben reunir los espacios de datos para garantizar su interoperabilidad, su gobernanza y su sostenibilidad. El presente marco desarrolla dichos principios desde la perspectiva estrictamente técnica, centrándose en arquitecturas, componentes y mecanismos que pueden implementarse en cualquier dominio.

Asimismo, el documento incorpora las obligaciones y requisitos derivados del Data Act, el Data Governance Act, el Reglamento Europa Interoperable, del RGPD y del ENS, asegurando que los mecanismos técnicos aquí descritos son coherentes con los requisitos normativos europeos en materia de acceso, uso, intercambio, protección y portabilidad de datos.

1.4. Marco de interoperabilidad y recursos en desarrollo.

La selección de tecnologías y estándares incluida en esta versión del Marco Técnico de Interoperabilidad responde a criterios de madurez, estabilidad y alineación con los principios de interoperabilidad europeos así como las legislaciones pertinentes como el Data act o el Data Governance act, buscando proporcionar una base sólida y funcional para el despliegue de espacios de datos a nivel nacional.

Cabe precisar que iniciativas estratégicas como Simpl-Open, concebida para proporcionar un middleware interoperable que facilite la implementación de los servicios habilitadores aquí descritos, se encuentran todavía en fase de desarrollo. Por consiguiente, el detalle técnico de Simpl (junto con el de otras soluciones y protocolos innovadores que alcancen la madurez operativa necesaria), será incorporado y ampliado en futuras versiones de este documento, asegurando así que el marco evolucione en paralelo al estado del arte tecnológico y normativo tanto a nivel europeo como nacional.

En este sentido cabe destacar que en el contexto de la estrategia de la unión europea para la autonomía tecnológica del continente Simpl es una apuesta de la comisión europea para la creación de un ecosistema de datos y una economía del dato soberana en la que los estados miembros puedan participar en las mismas condiciones entre ellos.

1.5. Ecosistemas de valor habilitados por los espacios de datos

Los espacios de datos no son únicamente infraestructuras técnicas, son mecanismos para generar valor económico, social y estratégico a partir de la compartición segura y gobernada de información entre organizaciones públicas y privadas. Su propósito fundamental es habilitar un ecosistema en el que múltiples actores puedan colaborar, innovar y crear nuevos servicios basados en datos sin perder el control sobre sus activos.

En este ecosistema, la plataforma de interoperabilidad central – definida en este Marco de Interoperabilidad técnica – actúa como la pieza clave que permite que los espacios de datos funcionen. Sobre esta plataforma común se construyen soluciones y capacidades que impulsan:

- El desarrollo de casos de uso sectoriales (energía, salud, turismo, movilidad, etc.)
- La creación de servicios públicos y privados basados en datos.
- La colaboración público-privada.
- La aparición de nuevos modelos de negocio y cadenas de valor.
- La capacidad de reutilizar datos de forma responsable y bajo soberanía.

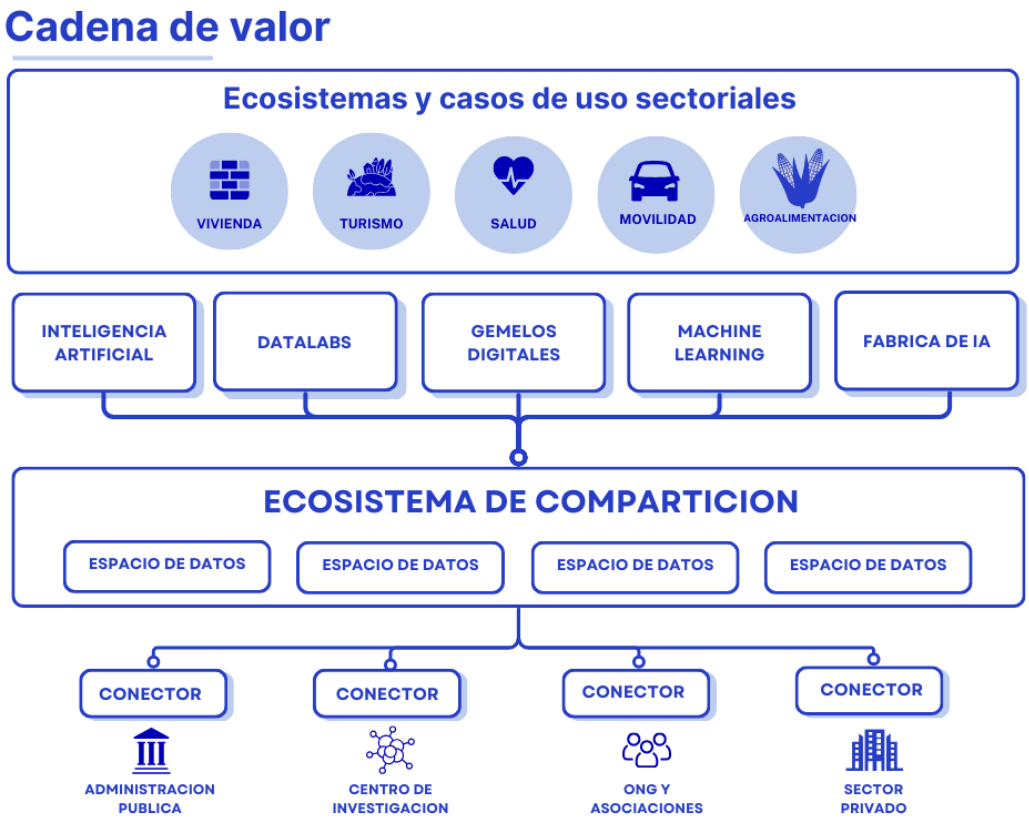


Ilustración 1: Cadena de valor

Gracias a esta capa de interoperabilidad, los participantes pueden conectar sus activos en un entorno más amplio, donde tecnologías como la analítica avanzada, IA, modelos predictivos, o los gemelos digitales pueden operar sobre información confiable procedente de múltiples dominios.

Asimismo, los espacios de datos sectoriales pueden federarse ente si, habilitando casos de uso intersectoriales – salud + movilidad, industria + energía – que requieren combinar información de ecosistemas tradicionalmente separados. Esta capacidad federada se convierte en un multiplicador de valor, permitiendo resolver problemas complejos y habilitar innovaciones que ninguna organización podía abordar de manera aislada.

En conjunto, este ecosistema de valor constituye el propósito final del Marco de Interoperabilidad Técnica, disponer de una base común que permita conectar datos, organizaciones y sectores, y apoyar así una economía del dato dinámica, competitiva y alineada con la visión europea.

1.6. Objetivos del Marco de Interoperabilidad

El Marco de Interoperabilidad Técnico tiene como objetivo proporcionar la infraestructura común que permita materializar el ecosistema de valor descrito en el apartado anterior.

Sus objetivos principales son:

- Definir los mecanismos técnicos esenciales que permiten la interoperabilidad primero entre participantes como aspecto prioritario, aportando también indicaciones en el ámbito entre varios espacios de datos.
- Establecer una arquitectura de referencia modular y escalable, alineada con estándares abiertos y principios de diseño interoperable.
- Proporcionar un conjunto mínimo de componentes funcionales, APIs y estándares necesarios para el intercambio seguro, confiable y gobernado de datos.
- Promover la soberanía del dato, asegurando que los participantes mantienen control sobre accesos, políticas, procesos y tecnologías utilizadas.
- Garantizar el cumplimiento normativo por diseño, integrando requisitos legales, de protección de datos, de seguridad y de auditoría en los mecanismos técnicos del espacio de datos.
- Facilitar la adopción de soluciones reutilizables a nivel europeo y asegurar la compatibilidad con los futuros espacios europeos de datos.

1.7. Alcance funcional y técnico

Este marco define los elementos técnicos necesarios para habilitar la interoperabilidad dentro de un espacio de datos y entre espacios de datos, incluyendo:

- Arquiteturas técnicas, componentes e interfaces.
- Mecanismos de adhesión, identificación y verificación de participantes.
- Publicación y gestión de catálogos de datos y servicios.
- Mecanismos de descubrimiento y acceso controlado.
- Procesos de negociación, contratación y gestión de políticas.
- Protocolos de transferencia y control en tiempo de intercambio.
- Mecanismos de validación, auditoría y trazabilidad.
- Infraestructura técnica de confianza, seguridad y protección de datos.

El marco no cubre la definición de:

- Modelos de negocio o estructuras económicas del espacio de datos
- Semántica sectorial específica, la definición de ontologías, vocabularios o modelos semánticos sectoriales.
- Procedimientos organizativos detallados más allá de los necesarios para soportar la infraestructura técnica.

1.8. Destinatarios y roles de aplicación

Este marco está dirigido a todas las entidades que participan en el diseño, despliegue, operación o supervisión de un espacio de datos, incluyendo:

- Autoridades de gobierno del espacio de datos: responsables de aplicar este marco como referencia técnica para el diseño y despliegue de sus espacios de datos.
- Operadores técnicos del espacio de datos: encargados de implementar, mantener y operar los componentes, servicios y sistemas necesarios.
- Proveedores de datos y servicios: quienes deben cumplir los requisitos técnicos para publicar, describir, negociar y compartir productos de datos.

- Consumidores de datos y servicios: participantes que acceden o reutilizan datos bajo mecanismos interoperables.
- Organismos auditores o certificadores: entidades que verifican la conformidad técnica y la interoperabilidad de los componentes.
- Administraciones públicas promotoras de espacios de datos: que requieren referencias homogéneas para garantizar la calidad y sostenibilidad del ecosistema.

1.9. Estructura del documento

El presente documento se organiza de forma progresiva para guiar al lector desde los fundamentos conceptuales de los espacios de datos hasta su aplicación técnica y normativa.

El Capítulo 1 presenta el contexto europeo y nacional que motiva la elaboración del MRT y sus objetivos.

El Capítulo 2 expone los fundamentos de la interoperabilidad en espacios de datos, definiendo las dimensiones, principios y bases conceptuales del Marco de Gobernanza y del Marco Técnico.

El Capítulo 3 desarrolla el Marco de Interoperabilidad Técnico, describiendo los componentes esenciales y los procesos operativos que permiten el intercambio de datos dentro y entre espacios de datos.

El Capítulo 4 sintetiza los requisitos técnicos normativos en formato esquemático y tabular, proporcionando la primera especificación de alto nivel para la validación de conformidad.

Los anexos abordan los elementos de gobernanza técnica, supervisión y mejora continua, complementados con un glosario y, en conjunto, la estructura del documento permite comprender, diseñar, implementar y evaluar espacios de datos interoperables conforme a los principios establecidos en la UNE 0087:2025.

2. Principios y fundamentos de la interoperabilidad

La interoperabilidad es el elemento que permite que un espacio de datos funcione como un sistema coherente y no como una suma de organizaciones y tecnologías aisladas. Gracias a la interoperabilidad, distintas entidades —con sus propios sistemas, modelos de datos, reglas internas y capacidades tecnológicas— pueden intercambiar información y aplicar un conjunto común de políticas, mecanismos de confianza y criterios técnicos, manteniendo siempre la soberanía sobre sus datos.

Este capítulo presenta los fundamentos conceptuales que explican qué significa interoperar en un espacio de datos y por qué esta capacidad es indispensable para generar valor económico y social a partir del intercambio de datos. No se describen aún componentes técnicos ni procesos detallados; esa labor corresponde al siguiente capítulo, que desarrolla el Marco Técnico de Interoperabilidad. Aquí abordamos, de forma teórica y comprensible:

- cómo se estructura un espacio de datos desde el punto de vista conceptual,
- qué papel desempeña la interoperabilidad en este tipo de ecosistemas,
- qué diferencias existen entre el espacio de datos como ecosistema y como plataforma técnica (Data Space Backbone),
- qué pilares conceptuales hacen posible el intercambio gobernado,

- y qué claves deben cumplirse para interoperar dentro de un ED y entre diferentes ED.

Este capítulo también integra qué funciones básicas deben estar presentes en cualquier espacio de datos —gestión de participantes, descripción de recursos, publicación, descubrimiento, negociación, intercambio y auditoría—, sin entrar en cómo se implementan.

El objetivo es proporcionar una base sólida, clara y comprensible que permita entender por qué en el Capítulo 3 existirán determinados componentes técnicos y cómo estos responden a las necesidades funcionales de un espacio de datos. Con ello, el lector queda preparado para transitar de la teoría a la solución técnica: del concepto al diseño, y del diseño a la implementación.

2.1. Qué entendemos por interoperabilidad en un espacio de datos

La interoperabilidad en un espacio de datos es la capacidad de que diferentes organizaciones —con sistemas, tecnologías, políticas y modelos de datos heterogéneos— puedan interactuar y compartir información de forma gobernada, segura y comprensible, sin necesidad de acuerdos bilaterales específicos ni integraciones ad-hoc. Es el mecanismo que permite que un espacio de datos funcione como una infraestructura coherente y reutilizable, en la que todos sus participantes pueden colaborar bajo las mismas reglas técnicas y organizativas.

A diferencia de otros modelos de integración tradicionales, donde cada organización debe adaptarse a las particularidades de sus contrapartes, en un espacio de datos la interoperabilidad se concibe como un bien común, articulado mediante un conjunto de principios, servicios y estándares que todos los participantes comparten. Gracias a ello, cualquier entidad puede publicar datos, descubrir recursos, negociar condiciones de acceso, solicitar un intercambio y generar evidencias del uso realizado siguiendo un modelo homogéneo y repetible, independientemente de su tamaño o de la tecnología que utilice internamente.

En el contexto de la UNE 0087:2025, esta interoperabilidad se articula en cuatro dimensiones esenciales que, actuando de forma conjunta, hacen posible el intercambio confiable de datos y la ejecución de procesos comunes entre participantes.

Desde una perspectiva de gobernanza, la interoperabilidad no puede entenderse como un elemento aislado, sino como un ámbito específico dentro de la gobernanza global del espacio de datos, estrechamente vinculado al ciclo de vida del ecosistema y a la gestión de dato. Para que las reglas, políticas y acuerdos definidos por los participantes puedan aplicarse de manera efectiva, la interoperabilidad debe integrarse de forma coherente con la gobernanza organizativa del espacio de datos y con la gobernanza del dato, actuando como el mecanismo que conecta ampos planos y los hace operativos en la práctica.

La siguiente ilustración sitúa la gobernanza de la interoperabilidad como un domino propio, diferenciado pero complementario, y muestra cómo sus distintas dimensiones permiten articular la interacción entre participantes, tanto dentro de un espacio de datos como en su relación con otros espacios de datos, a lo largo de todo el ciclo de vida.

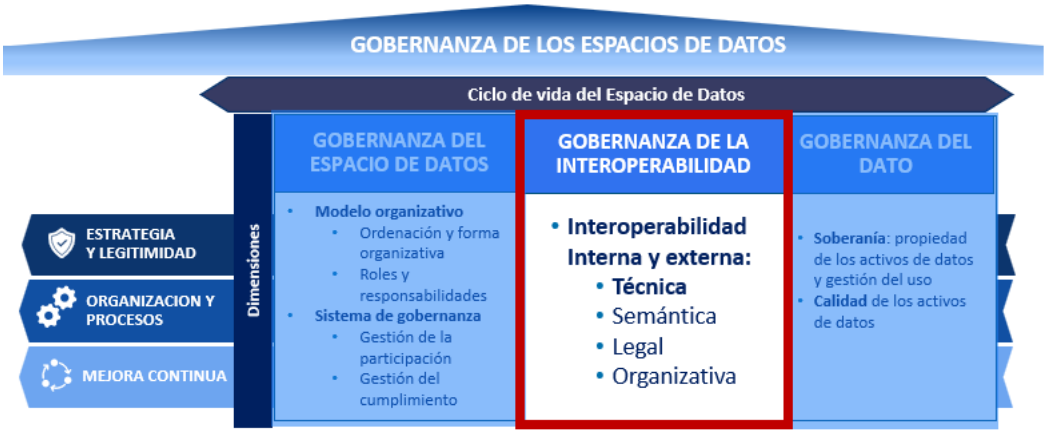


Ilustración 2: Gobernanza de los espacios de datos

Estas dimensiones no deben entenderse como capas aisladas, sino como los pilares conceptuales que sostienen la interacción en un espacio de datos y que permiten trasladar la gobernanza organizativa a su ejecución técnica.

a) Interoperabilidad legal

La interoperabilidad legal garantiza que todos los intercambios de datos se realizan dentro de un marco jurídico común, entendido y aceptado por los participantes. Incluye:

- el cumplimiento de la normativa aplicable al tratamiento y reutilización del dato,
- las obligaciones derivadas de la cesión o el acceso a la información,
- las licencias y restricciones legales aplicables a los recursos,
- las responsabilidades de proveedor y consumidor,
- y los mecanismos contractuales que regulan la relación entre las partes.

Sin esta dimensión, las organizaciones no pueden confiar en que sus derechos quedarán protegidos ni en que los datos se utilizarán conforme a las finalidades acordadas. La interoperabilidad legal es el fundamento de la confianza institucional en el espacio de datos.

b) Interoperabilidad organizativa

La interoperabilidad organizativa permite que entidades con diferentes estructuras internas, modelos de negocio y capacidades puedan coordinarse bajo reglas comunes. Esta dimensión define:

- los roles (proveedores, consumidores, operadores, intermediarios),
- las responsabilidades asociadas a cada rol,
- los mecanismos de adhesión, permanencia y suspensión,
- la gestión de políticas generales del espacio,
- y los procesos de cooperación y supervisión.

Gracias a esta dimensión, un espacio de datos puede escalar más allá de acuerdos bilaterales y convertirse en un ecosistema organizado, con reglas claras y predecibles que permiten que los procesos se ejecuten de forma uniforme.

c) Interoperabilidad semántica

La interoperabilidad semántica asegura que las organizaciones no solo puedan acceder a los datos, sino comprenderlos y reutilizarlos correctamente. Para ello, se apoya en la existencia de:

- metadatos estructurados y homogéneos,
- vocabularios y taxonomías compartidas,
- modelos conceptuales comunes,
- validación semántica,
- y criterios de calidad que permitan evaluar la fiabilidad de un recurso.

En esta dimensión, conceptos, elementos y estructuras utilizadas por diferentes organizaciones adquieren un significado compartido, imprescindible para evitar ambigüedades y garantizar que los datos puedan circular por toda la cadena de valor del ecosistema.

d) Interoperabilidad técnica

La interoperabilidad técnica es la dimensión que hace operativas las anteriores y permite que los participantes ejecuten interacciones reales: descubrir datos, validar identidades, negociar condiciones, transferir información y generar evidencias. Esta dimensión se materializa, entre otros elementos, en:

- interfaces comunes,
- mecanismos de autenticación y autorización,
- modelos de políticas legibles por máquina,
- formatos de representación estructurados,
- componentes compatibles entre organizaciones,
- y servicios compartidos que gestionan la interacción técnica.

Sin esta dimensión, las organizaciones podrían coincidir en los objetivos y en las reglas, pero no podrían llevar a la práctica el intercambio de datos. La interoperabilidad técnica es la que convierte el espacio de datos en infraestructura operativa, capaz de ejecutar procesos con garantías de seguridad, fiabilidad y trazabilidad.

2.2. El espacio de datos como marco de gobernanza y como marco técnico

Un espacio de datos puede entenderse desde dos perspectivas complementarias: como marco de gobernanza y como marco técnico. Esta distinción es fundamental para comprender cómo se organiza la interoperabilidad y por qué es necesario disponer de un marco técnico común para que los procesos funcionen de manera coherente entre organizaciones y sectores.

1. El espacio de datos como marco de gobernanza

En su dimensión más amplia, un espacio de datos es un marco de gobernanza de colaboración en el que organizaciones públicas y privadas comparten datos para generar valor económico y social. Esta colaboración se articula a través de un marco común que establece:

- roles (proveedor, consumidor, intermediario, operador, autoridad de gobernanza),
- responsabilidades,
- políticas generales del espacio,
- acuerdos legales y contractuales,

- incentivos que justifican la participación,
- mecanismos de supervisión y confianza.

Este nivel de gobernanza define el para qué y el cómo se organiza el espacio de datos.

Según la UNE 0087:2025, este marco corresponde a las dimensiones legal y organizativa de la interoperabilidad, que permiten que distintas organizaciones colaboren bajo un marco común, predecible y transparente.

El marco de gobernanza es, por tanto, la capa donde se da sentido al intercambio de datos; donde se define qué se espera de cada participante y cómo se garantiza que el valor generado revierte en todos los actores del espacio.

2. El espacio de datos como marco técnico

Para que ese ecosistema pueda funcionar, es necesario un conjunto mínimo de capacidades técnicas comunes que permitan que las interacciones se ejecuten de forma segura, homogénea y verificable. Esta es la dimensión que denominamos marco técnico del espacio de datos.

El marco técnico no sustituye los sistemas internos de las organizaciones, sino que actúa como la infraestructura compartida de interoperabilidad, proporcionando servicios que todos necesitan para interactuar:

- Identidad y atributos verificables, para garantizar autenticidad y atribución.
- Registro de participantes, como fuente de verdad sobre quién forma parte del ecosistema y en qué condiciones.
- Catálogo de recursos, donde los proveedores describen sus activos mediante metadatos estructurados.
- Biblioteca de vocabularios, que da coherencia semántica al ecosistema.
- Motor de políticas, que evalúa automáticamente condiciones de acceso y uso.
- Conectores, que ejecutan la interacción técnica entre organizaciones.
- Observabilidad y auditoría, para recopilar evidencias y garantizar cumplimiento.

En términos de la UNE 0087:2025, esta plataforma materializa la dimensión técnica de la interoperabilidad, haciendo operativas las reglas legales, organizativas y semánticas.

3. Por qué es necesario separar el marco de gobernanza y el marco técnico

Separarlas conceptualmente permite:

- explicar mejor por qué existen ciertos componentes técnicos,
- reconocer que los casos de uso o modelos de negocio pueden variar mientras la plataforma técnica permanece estable,
- garantizar que los espacios de datos son compatibles entre sí, aunque sus gobernanzas sean distintas,
- facilitar la integración entre ED sectoriales o territoriales.

El marco de gobernanza define el contexto de colaboración, el marco técnico define cómo se hace posible esa colaboración.

4. Cómo se relacionan ambas capas en la práctica

Las dos dimensiones actúan de forma complementaria:

- El marco de gobernanza establece las reglas, los incentivos y las condiciones legales u organizativas.
- El marco técnico aplica esas reglas mediante mecanismos verificables:
  - validación de identidades,
  - descubrimiento de recursos,
  - ejecución de políticas,
  - negociación de contratos,
  - transferencia segura,
  - trazabilidad y evidencias.

2.3. Interoperabilidad dentro del espacio de datos y entre espacios de datos

La interoperabilidad en un espacio de datos no se limita a permitir el intercambio entre organizaciones que pertenecen al mismo ecosistema. Para que los espacios de datos cumplan su propósito estratégico —facilitar la economía del dato, habilitar nuevos servicios digitales y permitir la colaboración entre dominios— deben ser capaces de operar tanto internamente como de manera federada con otros espacios de datos.

Esta sección explica, desde una perspectiva conceptual, los dos niveles de interoperabilidad que deben gestionarse en un espacio de datos y constituye uno de los elementos clave de la UNE 0087:2025 al definir un ecosistema que puede escalar y conectarse con otros entornos.

1. Interoperabilidad dentro del espacio de datos

La interoperabilidad interna se refiere a la capacidad de los participantes de un mismo espacio de datos para:

- describir sus activos utilizando un lenguaje común,
- descubrir los datos publicados por otros participantes,
- interpretar correctamente las políticas y condiciones asociadas al uso del dato,
- negociar acuerdos en base a reglas homogéneas,
- transferir datos de forma segura,
- y generar evidencias verificables de cada interacción.

Este nivel de interoperabilidad exige que el Marco de Gobernanza y el Marco Técnico se apliquen de forma coherente y uniforme a todos los participantes.

Conceptualmente, esta interoperabilidad interna permite:

- que el proveedor tenga la seguridad de que su dato será usado conforme a sus políticas,
- que el consumidor entienda de forma inequívoca qué puede esperar del recurso,
- que los procesos (publicación, descubrimiento, negociación y transferencia) funcionen siempre igual,
- que las evidencias se generen de forma sistemática,
- y que el espacio de datos funcione como un entorno confiable para todos sus actores.

Este nivel de interoperabilidad se refleja en funciones como:

- gestión de vocabularios y metadatos comunes,
- catalogación y descubrimiento,
- definición y evaluación de políticas,
- intercambio gobernado de datos,
- y observabilidad del uso.

2. Interoperabilidad entre espacios de datos

Más allá del funcionamiento interno, y si su propósito así lo requiere, un espacio de datos debería ser capaz de interoperar con otros espacios de datos, independientemente de:

- su dominio sectorial,
- su modelo organizativo,
- su tecnología,
- su nivel de madurez.

Esta interoperabilidad federada es esencial para:

- conectar cadenas de valor completas (p. ej., energía ↔ movilidad ↔ industria),
- habilitar servicios públicos digitales basados en múltiples fuentes,
- facilitar la innovación multisectorial,
- escalar casos de uso más allá de un único ámbito organizativo,
- y garantizar que los datos pueden circular allí donde crean mayor valor.

Conceptualmente, la interoperabilidad entre espacios de datos requiere:

- acuerdos de reconocimiento mutuo del Marco de Gobernanza,
- modelos de identidad y atributos compatibles,
- semánticas interoperables basadas en vocabularios compartidos o federados,
- políticas legibles por máquina que puedan evaluarse en ambos espacios,
- y procesos comunes para negociar y autorizar el intercambio entre espacios.

Este nivel de interoperabilidad no implica uniformidad entre espacios, sino compatibilidad, basada en la existencia de principios conceptuales y técnicos compartidos.

La UNE 0087:2025 reconoce esta necesidad cuando define espacios de datos capaces de conectarse a otros ecosistemas manteniendo su autonomía organizativa y de gobernanza.

3. Relación entre ambos niveles de interoperabilidad

Los dos niveles —interno y federado— son complementarios:

- La interoperabilidad interna garantiza el funcionamiento homogéneo dentro del espacio.
- La interoperabilidad federada permite su expansión, conexión y escalabilidad.

Para que exista interoperabilidad entre espacios, primero debe existir interoperabilidad dentro de cada espacio. Por eso, el Marco Técnico se construye de forma modular, reutilizable y basada en principios comunes que puedan extenderse a otros contextos.

Esta visión permite:

- que distintos sectores adopten el Marco Técnico sin perder autonomía,
- que se creen espacios de datos especializados (energía, turismo, sanidad, industria...)
- que dichos espacios puedan federarse cuando sus usos lo requieran,
- y que la economía del dato en España evolucione como un ecosistema interconectado.

2.4. Capacidades funcionales esenciales en los espacios de datos

Las cuatro dimensiones de interoperabilidad descritas en la norma UNE 0087:2025 (legal, organizativa, semántica y técnica) se materializan, a nivel funcional, en una serie de capacidades básicas que todo espacio de datos debe habilitar para que sus participantes puedan operar de forma coherente, segura y orientada al valor.

Existen un conjunto estable de funciones que deben aparecer en cualquier espacio de datos, independientemente de su tamaño, dominio o grado de madurez.

Ilustración 3: Capacidades funcionales esenciales

1. Gestión de participantes y del marco de gobernanza

Todo espacio de datos necesita gestionar de forma estructurada:

- la incorporación de nuevos participantes,
- la asignación de roles,
- la verificación de identidades y atributos,
- el mantenimiento del estado operativo de cada actor,
- y la aplicación del marco de gobernanza en términos de responsabilidades, obligaciones y reglas de comportamiento.

Conceptualmente, esta capacidad sostiene la interoperabilidad legal y organizativa del ecosistema.

2. **Descripción, publicación y mantenimiento de los recursos de datos**

Para poder descubrir e intercambiar datos, es necesario que los proveedores puedan:

- describir sus activos mediante metadatos estructurados,
- emplear vocabularios y modelos semánticos compartidos,
- asociar políticas de uso a sus recursos,
- versionar y actualizar la información publicada,
- y retirar los recursos cuando corresponda.

Estas funciones habilitan la interoperabilidad semántica y permiten que los consumidores comprendan, evalúen y reutilicen los datos ofrecidos por otros participantes.

3. **Descubrimiento y evaluación de recursos**

Los consumidores deben contar con mecanismos que les permitan:

- buscar y filtrar activos relevantes,
- comprender las características técnicas y semánticas de los recursos,
- interpretar las políticas de uso,
- y determinar si un recurso es adecuado para su propósito.

Esta capacidad es esencial para articular procesos de negociación posteriores y para asegurar que los intercambios se realizan de forma informada.

4. **Negociación de condiciones de acceso y uso**

Un espacio de datos debe ofrecer una forma coherente, transparente y reproducible de:

- solicitar acceso a un recurso,
- evaluar condiciones de uso,
- proponer y recibir ofertas,
- aceptar o rechazar acuerdos,
- y formalizar un contrato vinculante entre proveedor y consumidor.

Esta función se basa en las dimensiones legal, organizativa y técnica de la interoperabilidad, ya que combina reglas de gobernanza con mecanismos de evaluación automática de políticas.

5. **Intercambio gobernado de datos**

La transferencia de datos entre participantes requiere capacidades que permitan:

- autorizar o denegar el acceso conforme al contrato,
- aplicar restricciones durante la transmisión,
- utilizar canales seguros,
- verificar identidades y atributos,
- y garantizar que el proveedor mantiene la soberanía sobre el dato en todo momento.

Esta función es la esencia de la interoperabilidad técnica aplicada a procesos reales.

6. **Observabilidad, auditoría y trazabilidad**

Para mantener un entorno confiable, todo espacio de datos debe poder:

- registrar las interacciones realizadas por los participantes,
- generar evidencias verificables sobre el uso del dato,
- supervisar el comportamiento del ecosistema,
- detectar incidencias,
- y facilitar auditorías internas o externas.

Esta capacidad garantiza la responsabilidad, el cumplimiento y el ciclo de vida completo del dato.

7. **Capacidad de federación con otros espacios de datos**

Más allá de la interacción interna, un espacio de datos debe estar preparado para:

- conectar catálogos,
- intercambiar vocabularios,
- reconocer identidades,
- evaluar políticas entre dominios,
- y habilitar procesos de intercambio entre ED.

Esta funcionalidad es esencial para la escalabilidad del ecosistema y para cumplir con la visión europea de un mercado único de datos.

Con esta base conceptual, el documento está en condiciones de avanzar desde el qué y el por qué hacia el cómo. El capítulo siguiente describe el Marco Técnico de Interoperabilidad, donde se detallarán:

- los componentes comunes que deben existir en la plataforma técnica de un espacio de datos,
- las funciones que debe ofrecer cada uno,
- las interacciones que permiten ejecutar los flujos operativos,
  y la forma en que estos componentes materializan las cuatro dimensiones de interoperabilidad descritas en este capítulo.

3. Marco de Interoperabilidad Técnico

El Marco de Interoperabilidad Técnico define los componentes, servicios, interfaces y mecanismos comunes que permiten a los participantes de un espacio de datos ejecutar los procesos fundamentales de publicación, descubrimiento, negociación, intercambio y supervisión de datos. Si el capítulo anterior ha establecido los fundamentos conceptuales sobre qué significa interoperar en un espacio de datos, este capítulo concreto cómo se habilita esa interoperabilidad en la práctica, proporcionando un modelo claro, modular y adoptable para su implementación.

Según la UNE 0087:2025, el espacio de datos requiere un marco técnico que permita materializar las dimensiones legal, organizativa, semántica y técnica de la interoperabilidad mediante mecanismos automatizables y verificables. Esto implica disponer de un conjunto común de servicios habilitadores que todos los participantes

deben conocer y utilizar, garantizando así que las interacciones siguen un patrón homogéneo y que las reglas del Marco de Gobernanza pueden aplicarse de forma sistemática.

Este capítulo presenta dicho marco técnico desde dos perspectivas complementarias:

1. **Los componentes comunes del espacio de datos**

Esta primera parte describe los servicios esenciales que constituyen la base técnica de un espacio de datos, independientemente del sector, caso de uso o tecnología utilizada internamente por las organizaciones.

Estos componentes incluyen, entre otros:

- Gestión de identidad y atributos verificables
- Registro de participantes
- Catálogo de recursos
- Biblioteca de vocabularios y mecanismos de semántica
- Motor de políticas y mecanismos de autorización
- Conector de interoperabilidad entre organizaciones
- Observabilidad y auditoría técnica

Cada componente será presentado de forma estructurada, describiendo:

- su propósito,
- las funciones que debe cumplir,
- las interacciones que soporta,
- su aportación a la interoperabilidad,
- y su relación con los flujos operativos.

Este enfoque responde a uno de los principales retos señalados por el ecosistema: la necesidad de disponer de una arquitectura mínima común, comprensible, replicable y preparada para ser implementada por proyectos financiados, proveedores tecnológicos y administraciones públicas.

2. **La interacción entre componentes: los procesos técnicos del espacio de datos**

La segunda parte del capítulo describe cómo estos componentes trabajan conjuntamente para habilitar los procesos clave del espacio de datos, concretamente:

- la adhesión y activación de participantes,
- la publicación y puesta a disposición de recursos,
- el descubrimiento y evaluación por parte de los consumidores,
- la negociación y formalización de condiciones de uso,
- la transferencia gobernada de datos,
- y la generación de evidencias para auditoría.

Esta estructura permite que el lector comprenda, de forma clara y visual, cómo se relacionan los servicios del Marco Técnico y por qué cada uno de ellos es indispensable para ejecutar los procesos mínimos definidos en el MRT.

3.1. Visión general del Marco de Interoperabilidad Técnico (explicación de la arquitectura general)

El Marco de Interoperabilidad Técnico define el conjunto de componentes, servicios comunes, interfaces y reglas operativas que permiten que un espacio de datos funcione de manera homogénea, segura y verificable. Su función es materializar, en términos técnicos, las dimensiones legal, organizativa, semántica y técnica definidas en la UNE 0087:2025, garantizando que las reglas del Marco de Gobernanza puedan ejecutarse de forma coherente por todos los participantes.

Esta arquitectura no sustituye los sistemas internos de las organizaciones, sino que actúa como una capa común que permite que estos sistemas interactúen bajo un marco uniforme, reduciendo la complejidad técnica y evitando integraciones ad-hoc.

1. **Una arquitectura modular basada en servicios habilitadores comunes**

El Marco Técnico se organiza en torno a un conjunto de servicios habilitadores que proporcionan capacidades transversales al ecosistema. Estos servicios permiten:

- identificar a los participantes de forma verificable,
- registrar sus atributos y roles,
- describir los activos de manera estructurada,
- aplicar políticas de acceso y uso,
- negociar y autorizar el intercambio de datos,
- realizar la transferencia de forma segura,
- y generar evidencias que permitan trazabilidad y auditoría.

Este conjunto de servicios habilitadores puede ser implementado mediante soluciones de middleware interoperable alineadas con iniciativas europeas como SIMPL-Open, que proporciona capacidades reutilizables para la gestión de identidad, catálogos, políticas y conectores en espacios de datos federados.

Estos servicios conforman la infraestructura técnica mínima de un espacio de datos. Su objetivo no es uniformizar tecnologías, sino normalizar las interfaces y procesos esenciales que permiten que los distintos participantes puedan operar bajo un mismo marco técnico.

La arquitectura técnica del espacio de datos define cómo se organizan los componentes y servicios que habilitan la interoperabilidad entre participantes. Su función es garantizar que todos los elementos del ecosistema - desde la gestión de identidades hasta la transferencia de datos - operen sobre una base tecnológica común, modular y verificable. De acuerdo con la UNE 0087:2025, esta arquitectura debe permitir la aplicación efectiva de las políticas del espacio de datos, la trazabilidad completa de las operaciones, la protección de la soberanía del dato y la supervisión continua del comportamiento del ecosistema.

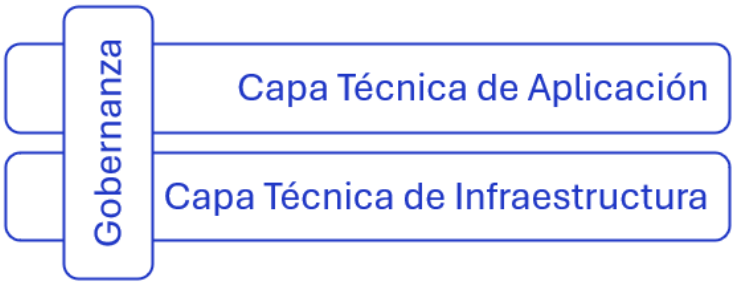


Ilustración 4:

El diseño se estructura en tres capas complementarias, cada una con responsabilidades específicas:

a) Capa de Aplicación

Incluye las interfaces y servicios a través de los cuales los participantes interactúan con el espacio de datos: portales, paneles de operación, APIs de publicación y descubrimiento, herramientas de gestión de identidades y servicios de negociación. Esta capa garantiza una experiencia homogénea e independiente de la tecnología interna de cada organización, apoyándose en estándares abiertos como DCAT-AP, ODRL, RDF, JSON-LD o los modelos de identidad W3C. Esta aproximación se alinea con el European Interoperability Framework (EIF), que promueve modularidad y neutralidad tecnológica.

b) Capa de Infraestructura

Proporciona los elementos técnicos necesarios para la operación segura y resiliente del ecosistema: comunicaciones cifradas, almacenamiento bajo control del participante, orquestación de servicios, disponibilidad, redundancia y continuidad operativa. Esta capa asegura que la información no abandona los dominios técnicos del participante salvo cuando exista un contrato válido y una transferencia autorizada, en coherencia con los principios de soberanía recogidos en la UNE 0087:2025, el ENI, el ENS, el DGA y el Data Act.

c) Capa de Gobernanza Técnica

Traduce las políticas organizativas y contractuales en mecanismos operativos: autenticación, autorización, validación de credenciales, evaluación de políticas de uso, registro de operaciones y generación de evidencias. Esta capa garantiza que todas las interacciones del espacio de datos son coherentes, auditables y verificables.

Esta arquitectura en capas proporciona la base lógica para los componentes del Marco Técnico descritos a continuación y permite que la interoperabilidad se mantenga incluso cuando evolucionan tecnologías, participantes o casos de uso.

2. Integración con marcos europeos de referencia (EIRA y eGovERA)

La estructura del Marco Técnico de Interoperabilidad no parte de cero. Se apoya en marcos arquitectónicos europeos consolidados, como el *European Interoperability Reference*

Architecture (EIRA) y su extensión eGovERA, ampliamente utilizados en el desarrollo de servicios públicos digitales interoperables.

La acción de Interoperability Architecture Solutions, donde se desarrollan ambas soluciones EIRA y eGovERA, es una acción de la Comisión Europea que tiene como objetivo dar soporte a la creación de servicios públicos digitales interoperables desde el diseño. Ambas soluciones, EIRA y eGovERA, son recursos provistos por la comisión, que están disponibles para su reúso.

EIRA proporciona un marco de referencia común basado en building blocks reutilizables y en una arquitectura modular basada en el EIF, y que distingue claramente entre capas organizativas, semánticas, técnicas y de gobernanza. Esta aproximación respalda el diseño del presente Marco Técnico, al promover:

- la modularidad en los componentes del espacio de datos,
- la separación lógica entre el Marco de Gobernanza y el Marco Técnico,
- la definición de servicios habilitadores comunes,
- y la neutralidad tecnológica necesaria para permitir múltiples implementaciones compatibles.

Por su parte, eGovERA aporta un doble valor a los espacios de datos. En el plano funcional, proporciona una arquitectura de referencia que estructura los componentes técnicos, sus interacciones y las capacidades necesarias para implementar servicios digitales interoperables. En el plano organizativo, ofrece un enfoque estructurado para articular roles, responsabilidades y mecanismos de control en sistemas complejos. Esta doble contribución permite que el Marco Técnico del espacio de datos se refuerce tanto en su dimensión de arquitectura de solución (qué componentes y capacidades se necesitan) como en su relación con el Marco de Gobernanza (quién los gestiona y cómo se supervisan), garantizando un alineamiento coherente entre las estructuras tecnológicas y organizativas.

El MRT adopta sus principios como referencias arquitectónicas que contribuyen a que los espacios de datos españoles sean coherentes con las prácticas europeas, compatibles con otras iniciativas públicas y preparados para integrarse en un ecosistema de servicios y plataformas interoperables a escala nacional y europea.

3. Relación entre los servicios del Marco Técnico y los procesos del espacio de datos

Cada uno de los servicios comunes del Marco Técnico da soporte directo a los procesos funcionales y a los flujos mínimos de interoperabilidad.

En términos generales:

- La gestión de identidad y atributos habilita la adhesión, la autenticación y la autorización.
- El registro de participantes actúa como la fuente única de verdad sobre quiénes participan y en qué condiciones.
- El catálogo de recursos hace posible la descripción, descubrimiento y evaluación de activos.

- La biblioteca de vocabularios soporta la interoperabilidad semántica descrita en la UNE 0087:2025.
- El motor de políticas permite evaluar automáticamente permisos, prohibiciones y obligaciones.
- El conector ejecuta la interacción técnica entre organizaciones.
- La observabilidad permite supervisar el comportamiento técnico y generar evidencias verificables.

De este modo, el Marco Técnico proporciona la base operativa sobre la que se ejecutan todos los procesos del espacio de datos: publicación, descubrimiento, negociación, transferencia y auditoría.

4. Un marco neutral, reproducible y preparado para la federación

El Marco Técnico se diseña con cuatro objetivos estratégicos:

- Neutralidad tecnológica

Los componentes y servicios del marco no imponen tecnologías concretas, sino que definen requisitos funcionales e interfaces abiertas que pueden implementarse mediante diversas soluciones.

- Reproducibilidad

Los espacios de datos deben poder desplegarse de forma consistente en distintos sectores y proyectos, reutilizando patrones técnicos comunes.

- Interoperabilidad entre espacios de datos

El marco no solo habilita que organizaciones dentro del mismo ED interactúen, sino que varios ED puedan federarse, compartiendo vocabularios, catálogos, identidad y procesos compatibles.

- Preparación para certificación y pruebas

El Marco Técnico se estructura de forma que se pueda evaluar si una implementación cumple los requisitos mínimos para ser interoperable.

5. Componentes esenciales del Marco Técnico

El Marco Técnico se articula en torno a un conjunto de componentes comunes, que se describirán en detalle en los siguientes apartados:

- Gestión de identidad y atributos verificables
- Registro de participantes
- Catálogo de recursos
- Biblioteca de vocabularios
- Motor de políticas y autorización
- Conector de interoperabilidad
- Mecanismos de observabilidad y auditoría
- Servicios auxiliares y capacidades de integración

Estos componentes actúan como piezas de un sistema modular que puede adaptarse a las necesidades de cada espacio de datos, siempre que se mantengan las interfaces y comportamientos definidos.

3.2. Principios de diseño técnico

Los principios de diseño técnico constituyen las directrices que deben guiar la implantación de los componentes y servicios del espacio de datos, garantizando que la arquitectura resultante sea interoperable, segura, modular y conforme a los requisitos establecidos en el marco de gobernanza.

Para garantizar el desarrollo satisfactorio del espacio de datos, es esencial respetar e implementar los principios básicos como son: modularidad, escalabilidad, portabilidad y desacoplamiento.

- **Modularidad:** hace referencia a la división de los componentes que conforman un sistema, en este caso, el espacio de datos. De esta forma, los diferentes componentes pueden desarrollarse y estandarizarse de forma independiente, sin que se añadan dependencias.
- **Escalabilidad:** se trata de un principio básico para garantizar el correcto desarrollo del espacio de datos y de su ciclo de vida. El diseño de los diferentes componentes debe tener como base, la capacidad de ser escalado en las diferentes dimensiones: vertical, horizontal y elasticidad.
- **Portabilidad:** dando soporte al uno de los pilares de los espacios de datos, la portabilidad es un elemento clave para garantizar la soberanía digital del espacio de datos. Este principio se centra en asegurar que los diferentes componentes y soluciones desplegados puedan mantener la actividad independientemente del entorno en el que se desplieguen, asegurando la continuidad del servicio, y evitando la dependencia tecnológica.
- **Desacoplamiento:** Este principio permite el desarrollo de los componentes esenciales de forma independiente. Los diferentes componentes de un sistema tienen funciones y responsabilidades específicas, lo que es clave para garantizar que los componentes puedan ser desarrollados y provistos por diferentes agentes, garantizando su interoperabilidad y funcionamiento.

3.3. Componentes del Marco de Interoperabilidad Técnico

La interoperabilidad del espacio de datos no se alcanza únicamente definiendo principios o procesos, requiere de la existencia de un conjunto común de componentes técnicos capaces de ejecutar, de forma homogénea y verificable, las reglas establecidas en el Marco de Gobernanza y los procesos operativos del ecosistema. Estos componentes constituyen el núcleo del Marco Técnico y proporcionan las capacidades esenciales que permiten a los participantes publicar y descubrir activos, negociar condiciones de uso, intercambiar información de forma segura y generar evidencias trazables de todas sus acciones.

La UNE 0087:2025 establece que todo espacio de datos debe contar con servicios habilitadores mínimos para garantizar las cuatro dimensiones de interoperabilidad: legal, organizativa, semántica y técnica. Los componentes descritos en este bloque responden exactamente a esta necesidad. Cada uno cumple una función diferenciada – gestionar identidades, registrar participantes, describir activos, aplicar políticas, orquestar la interacción técnica o asegurar la trazabilidad –, pero todos interactúan para formar una plataforma técnica coherente, que permite que organizaciones heterogéneas colaboren bajo un marco común.

Los componentes descritos en este apartado son conceptualmente compatibles con las arquitecturas de referencia promovidas a nivel europeo para espacios de datos, incluyendo implementaciones basadas en Eclipse Dataspace Components (EDC) y su evolución dentro de iniciativas como SIMPL-Open.

Ilustración 5: Diagrama de componentes funcionales esenciales

En las secciones siguientes se presentan estos componentes de manera estructurada, explicando para cada uno:

- Su propósito dentro del espacio de datos.
- Las funciones que debe desempeñar.
- Los servicios técnicos que ofrece.
- Las interacciones que mantiene con otros componentes.
- Su contribución a la interoperabilidad global del ecosistema.

3.3.1. Servicio de Gestión de Identidad y atributos verificables

La gestión de identidad y atributos verificables es uno de los componentes esenciales del Marco Técnico del espacio de datos. Su función principal es asegurar que todos los participantes —organizaciones, usuarios delegados y componentes técnicos como conectores— puedan demostrar quiénes son, qué capacidades tienen y bajo qué legitimaciones pueden actuar dentro del espacio de datos.

Este componente hace operativos dos pilares conceptuales definidos en el Capítulo 2:

- la interoperabilidad legal y organizativa, al permitir asignar roles y responsabilidades verificables,
- y la interoperabilidad técnica, al proporcionar mecanismos de autenticación y autorización comunes para todos los participantes.

En la práctica, es el elemento que permite articular la confianza en el espacio de datos: sin identidades verificables y atributos certificados, los demás componentes no pueden aplicar políticas, autorizar solicitudes, negociar condiciones de uso ni garantizar que las interacciones se ejecutan de forma segura.

1. Descripción del componente

El componente de gestión de identidad y atributos verificables proporciona los servicios necesarios para:

- emitir,
- validar,
- revocar,
- y actualizar

las credenciales que representan a cada participante y a sus componentes técnicos.

Estas credenciales contienen atributos verificables, tales como:

- rol técnico (proveedor, consumidor, operador...),
- legitimación para actuar en nombre de la organización,
- permisos otorgados por el espacio de datos,
- características del conector utilizado,
- información relevante para evaluar políticas de acceso y uso.

Este componente no gestiona la identidad interna de cada organización, sino la identidad interoperable, es decir, la parte de la identidad que debe ser reconocida por todo el ecosistema.

2. Funciones principales

El componente cumple al menos las siguientes funciones:

1. Emisión de credenciales verificables

Permite que la autoridad responsable del espacio de datos emita credenciales digitales que certifican el rol, la legitimidad y los atributos del participante o del conector.

2. Validación de identidades

Ofrece mecanismos para verificar que una credencial presentada es auténtica, no ha sido modificada y sigue siendo válida.

3. Revocación y actualización

Permite invalidar credenciales comprometidas, caducadas o asociadas a participantes que han cambiado de rol o han dejado de cumplir condiciones del Marco de Gobernanza.

4. Pruebas criptográficas y presentación selectiva

Habilita a los participantes para presentar únicamente los atributos necesarios para una interacción, sin exponer información innecesaria.

5. Servicios para el resto de las componentes del ED

Los servicios de identidad son consumidos por el Registro de Participantes, el Motor de Políticas, el Catálogo y, de forma especialmente intensa, por los Conectores durante los flujos de negociación y transferencia.

Estas funciones permiten garantizar que todas las interacciones técnicas del espacio de datos se producen entre sujetos verificables y autorizados.

3. Servicios técnicos ofrecidos

Aunque cada implementación puede variar, el componente ofrece un conjunto común de servicios accesibles mediante APIs:

Ilustración 6: Componentes funcionales del servicio de gestión de identidad

- Servicio de emisión de credenciales. Para generar nuevas credenciales verificables.
- Servicio de validación. Para comprobar autenticidad, vigencia y firma de una credencial.
- Servicio de revocación y estado. Para consultar si una credencial sigue siendo válida o ha sido retirada.
- Servicio de introspección de atributos. Permite a otros componentes recuperar atributos necesarios para evaluar políticas.

- Servicio de registro de identidades. Coordina con el Registro de Participantes la inscripción del estado de cada identidad.
- Servicio de vinculación con conectores. Gestiona las identidades técnicas asociadas a conectores certificados.

Estos servicios no definen una implementación, pero sí establecen el mínimo funcional común para interoperar.

4. Interacciones principales con otros componentes

El componente de identidad interactúa con:

Ilustración 7: Interacciones principales del servicio de gestión de identidad

- Registro de Participantes (3.3)
  - Registra el estado, roles y atributos del participante.
  - Informa de altas, bajas, suspensiones y revocaciones.
- Catálogo (3.4)
  - Facilita información sobre el proveedor (identidad, rol) asociada a cada activo.
  - Permite evaluar legitimación del consumidor para consultar descripciones completas.
- Motor de Políticas (3.6)
  - Proporciona atributos verificados necesarios para evaluar permisos, prohibiciones y obligaciones.

- Conector (3.7)
    - Punto crítico de interacción: el conector utiliza credenciales verificables para
    - autenticación mutua,
    - autorización previa al acceso,
    - negociación,
    - transferencia y
    - generación de evidencias.
- Observabilidad y auditoría (3.8)
    - Registra qué credenciales se han validado en cada interacción.

En conjunto, este componente articula toda la cadena lógica del ED: sin identidad verificable, no hay negociación; sin atributos verificados, no se pueden aplicar políticas; sin pruebas criptográficas, no hay evidencias confiables.

5. Aportación del componente a la interoperabilidad del ED

La gestión de identidad y atributos verificables contribuye directamente a:

- Interoperabilidad legal, permitiendo demostrar legitimidad y derechos.
- Interoperabilidad organizativa, vinculando roles y responsabilidades.
- Interoperabilidad semántica, al aportar atributos que enriquecen la interpretación de políticas.
- Interoperabilidad técnica, al permitir autenticación y autorización automáticas en todos los flujos.

3.3.2. Registro de participantes

El Registro de Participantes es el componente que actúa como fuente única de verdad sobre quién forma parte del espacio de datos, bajo qué condiciones y con qué capacidades verificadas. Constituye uno de los pilares esenciales del Marco Técnico, ya que permite garantizar que todas las interacciones – publicaciones, descubrimientos, negociaciones, transferencias y auditorías – se realizan exclusivamente entre entidades legítimas, autorizadas y correctamente identificadas.

Mientras que el componente de identidad gestiona la emisión y validación de credenciales verificables, el Registro es el lugar donde se consolida esa información y donde se mantiene el estado administrativo y operativo de cada participante dentro del ED.

1. Descripción del componente

El Registro de Participantes almacena:

- la identidad verificable de cada entidad adherida.
- los roles técnicos asignados.
- los atributos certificados relevantes para evaluar políticas.
- el estado del participante (activo, suspendido, revocado, retirado).
- y las credenciales verificables emitidas y vigentes.

El Registro no gestiona información interna de cada organización, sino únicamente aquello que el ecosistema necesita para permitir una interacción interoperable y verificable.

Su existencia evita inconsistencias, duplicidades y comportamientos imprevisibles, al proporcionar a todos los componentes del espacio de datos un punto único de referencia sobre la legitimación de cada actor.

2. Funciones principales

El Registro cumple, al menos, las siguientes funciones:

1. Alta y activación de participantes

Registra a las entidades que han superado el proceso de adhesión y valida que su identidad y atributos coinciden con las credenciales emitidas.

2. Gestión del estado operativo

Permite activar, suspender temporalmente o retirar participantes del espacio de datos, según las reglas del Marco de Gobernanza.

3. Mantenimiento del historial de cambios

Conserva trazabilidad completa sobre modificaciones en roles, atributos e identidades, generando evidencias útiles para auditoría.

4. Publicación de atributos y legitimaciones

Pone a disposición del Motor de Políticas y de los Conectores los atributos necesarios para evaluar autorizaciones en los flujos del ED.

5. Coordinación con servicios de identidad

Actualiza automáticamente el estado de credenciales verificables revocadas o renovadas.

6. Provisión de información durante procesos operativos.

El Registro es consultado durante la publicación (para registrar proveedor), el descubrimiento (para exponer información básica), la negociación (para validar actores implicados) y la transferencia (para verificar vigencia).

3. Servicios técnicos ofrecidos

El Registro suele ofrecer servicios mediante APIs estandarizadas:

- Servicio de alta de participante. Incorpora una identidad validada al ED y registra su rol.
- Servicio de consulta de estado. Permite verificar si un participante está activo y bajo qué atributos.
- Servicio de actualización de roles y atributos. Gestiona cambios operativos que deben ser reflejados en todo el ecosistema.
- Servicio de revocación. Marca a un participante como no autorizado y notifica el resto de participantes.
- Servicio de auditoría. Permite consultar historiales de cambios y eventos relevantes.
- Servicio de sincronización con el componente de identidad. Para mantener coherencia entre credenciales emitidas y estado operativo.

Ilustración 8: Componentes fundamentales del registro de participante

4. Interacciones principales con otros componentes

El Registro se encuentra en el núcleo del Marco Técnico:

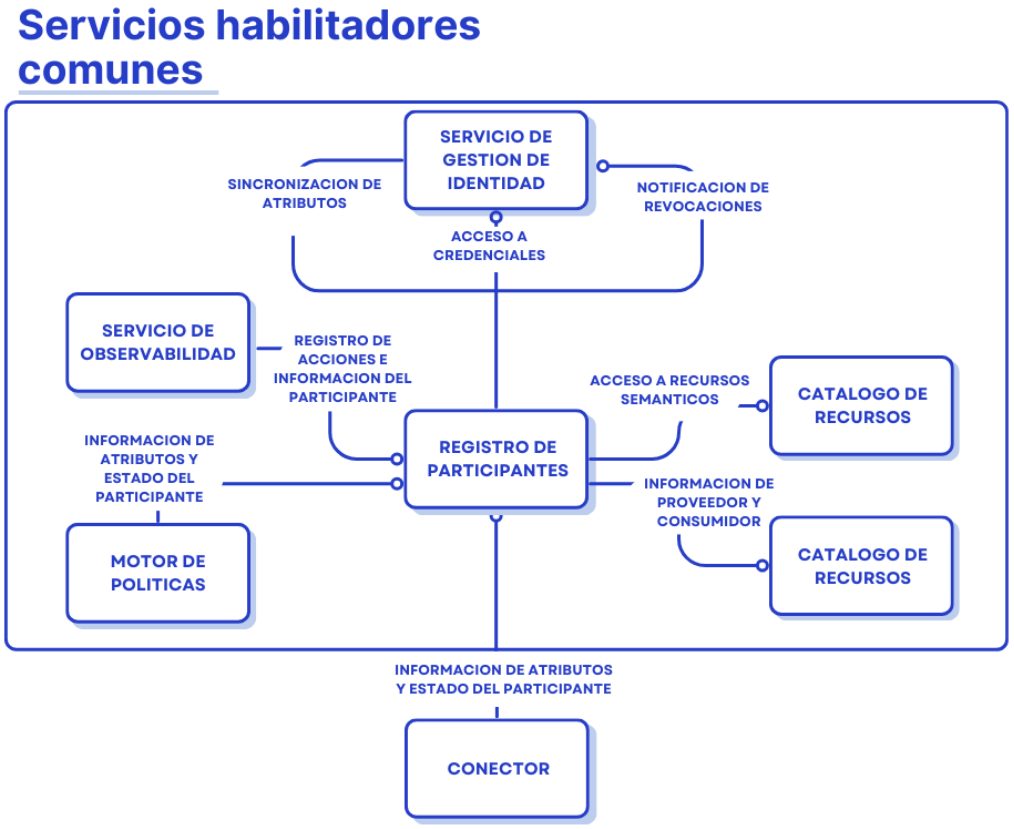


Ilustración 9: Interacciones principales del registro de participantes

- Identidad y atributos (3.2)
  - Recibe credenciales verificables emitidas.
  - Notifica revocaciones o suspensiones.
  - Sincroniza atributos certificados.
- Catálogo de recursos (3.4)
  - Aporta información validada del proveedor.
  - Proporciona información estructural del consumidor durante descubrimiento.
- Motor de Políticas (3.6)
  - Proporciona atributos para evaluar permisos y obligaciones.
  - Informa sobre el estado operativo del participante.
- Conector (3.7)
  - Valida identidad y rol del solicitante en negociación y transferencia.
  - Asegura que ningún actor no autorizado acceda a activos.
- Observabilidad (3.8)
  - Registra accesos al Registro y consultas realizadas.
  - Añade metainformación relevante al ciclo de auditoría.

Este nivel de interacción convierte al Registro en un componente transversal, sin el cual la interoperabilidad sería imposible.

5. **Aportación del componente a la interoperabilidad del ED**

El Registro contribuye simultáneamente a varias dimensiones:

- Interoperabilidad legal, garantiza legitimidad.
- Interoperabilidad organizativa, aplica roles y estados conforme al Marco de Gobernanza.
- Interoperabilidad semántica, facilita validaciones automáticas y consistentes.
- Interoperabilidad técnica, aporta atributos estructurados necesarios para aplicar políticas.

3.3.3. Catálogo de recursos

El Catálogo de Recursos es el componente encargado de gestionar y almacenar los metadatos descriptivos relativos a los activos disponibles en el espacio de datos. Su objetivo es permitir que los proveedores publiquen, describan y mantengan sus activos, y que los consumidores descubran, comprendan y evalúen dichos activos antes de iniciar cualquier proceso de negociación intercambio.

La construcción del catálogo puede materializarse de distintas formas, pudiendo constituirse como un componente centralizado que produzca, almacene y mantenga los metadatos de los activos, o también como una interfaz que garantice el acceso unificado a metadatos producidos, almacenados y mantenidos por uno o más sistemas distribuidos.

1. **Descripción del componente**

Los metadatos descriptivos deben ofrecer a los consumidores información suficiente para conocer:

- Qué activos existen.
- Quién los publica.
- Con qué restricciones.
- Bajo qué políticas de acceso y uso.
- Con qué nivel de calidad y completitud.
- Qué condiciones deben aceptarse para negociar su acceso y uso.

El Catálogo no aloja los datos, sino su representación estructurada, proporcionando el punto de referencia semántico, organizativo y operativo sobre el cual funcionan los procesos del espacio de datos.

2. Funciones principales

El Catálogo debe cumplir, como mínimo, las siguientes funciones:

1. Publicación de activos.

Permite a los proveedores registrar activos, entendidos como conjuntos de datos, distribuciones o servicios junto con sus metadatos, políticas y atributos de calidad.

2. Descubrimiento de activos.

Ofrece mecanismos de búsqueda, filtrado y consulta para que los consumidores puedan identificar recursos relevantes.

3. Evaluación previa del activo.

El consumidor debe poder comprender:

- La naturaleza del activo.
- La estructura y semántica de los recursos asociados.
- La calidad declarada (DQV).
- Su procedencia (PROV-O).
- Las políticas de uso aplicables (ODRL).
- Y las condiciones necesarias para su negociación.

4. Gestión del ciclo de vida.

Incluye creación, edición, versionado, actualización y retirada controlada de activos, preservando siempre la trazabilidad necesaria para auditoría.

5. Enlace con políticas.

Cada activo debe estar asociado a un conjunto de políticas legibles por máquina que serán evaluadas durante el proceso de negociación.

3. Servicios técnicos ofrecidos

El Catálogo proporciona los servicios necesarios para gestionar sus funciones internas, que suelen exponerse mediante APIs del espacio de datos.

Los componentes funcionales mínimos del Catálogo incluyen:

Ilustración 10: Componentes fundamentales del catálogo de recursos

Servicios incluidos:

- Servicio de creación y edición. Permite registrar y actualizar metadatos, vincular vocabularios y asociar políticas.
- Servicio de consulta. Ofrece búsquedas, filtrados y recuperación de fichas completas de los activos.
- Servicio de validación y control de calidad. Comprueba:
  - Conformidad con el perfil DCAT-AP adoptado.
  - Consistencia semántica usando vocabularios comunes.
  - Calidad declarada mediante DQV.
  - Integridad y coherencia de políticas ODRL.
- Servicio de persistencia. Gestiona el almacenamiento, versionado y estado de los metadatos del activo.
- Base de datos de metadatos. Repositorio estructurado donde se almacenan los registros del catálogo.

Para su construcción, el Catálogo implementa un perfil DCAT-AP adaptado convenientemente a las necesidades particulares del ecosistema en el que resida. Así mismo, los metadatos descriptivos deberán incluir un documento ODRL especificando el conjunto de políticas y restricciones aplicables, los detalles relativos a la calidad de este expresados usando el Data Quality Vocabulary, así como la información que permita identificar el linaje de los datos implementando PROV-O.

El diagrama a continuación ofrece una visión a alto nivel de los modelos de datos en base a los que se estructuran los metadatos del Catálogo:

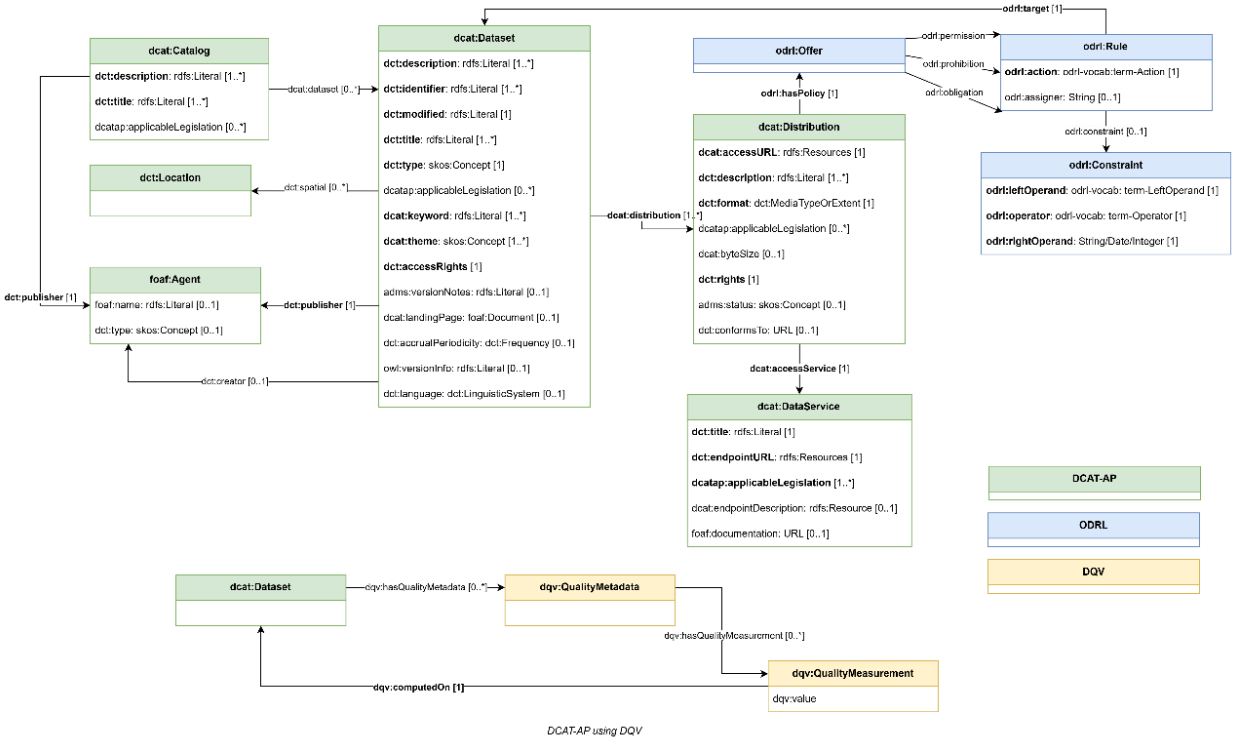


Ilustración 11: modelo de datos del Catálogo de Recursos.

Se presenta a continuación un ejemplo de una instancia de Dataset serializada en Turtle:

```
PREFIX dcat: <http://www.w3.org/ns/dcat#>
PREFIX dct:  <http://purl.org/dc/terms/>
PREFIX dcatap: <http://data.europa.eu/r5r/>
PREFIX odrl: <http://www.w3.org/ns/odrl/2/>
PREFIX rdf:  <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX time: <http://www.w3.org/2006/time#>

<https://datos.gob.es/catalogo>
  a dcat:Catalog ;
  dct:title "Catálogo de Datos Abiertos"@es, "Open Data Catalog"@en ;
  dct:description "Catálogo de Datos Abiertos del Gobierno de España"@es, "The Open Data Catalogue of the Government of Spain."@en ;
  dct:publisher <http://datos.gob.es/recurso/sector-publico/org/Organismo/E0DAT0001> .


<http://data.europa.eu/88u/dataset/0d24ea04-f026-4403-8df0-c9c6ff5174fd>
        rdf:type                dcat:Dataset;
        dct:accrualPeriodicity  <https://datos.gob.es/catalogo/a12002994-datos-de-calidad-del-aire1/Frequency>;
        dct:accessRights        <http://publications.europa.eu/resource/authority/access-right/PUBLIC>;
        dct:description         "A rede de Calidade do Aire pon a disposición do publico a posibilidade de consultar a información actual do Índice de Calidade do Aire (ICA)."@gl ;
        dct:identifier          "https://abertos.xunta.gal/catalogo/medio-ambiente/-/dataset/0055/datos-calidade-aire"^^<http://www.w3.org/2001/XMLSchema#anyURI>;
        dct:issued              "2012-02-08T00:00:00+01:00"^^<http://www.w3.org/2001/XMLSchema#dateTime>;
        dct:language            <http://publications.europa.eu/resource/authority/language/GLG> , <http://publications.europa.eu/resource/authority/language/SPA>;
        dct:modified            "2025-12-08T00:00:00+01:00"^^<http://www.w3.org/2001/XMLSchema#dateTime>;
        dct:publisher           <http://datos.gob.es/recurso/sector-publico/org/Organismo/A12002994>;
        dct:spatial             <http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Galicia>;
        dct:title               "Datos de calidad del aire"@es , "Air Quality data"@en;
        dcat:distribution       <http://data.europa.eu/88u/distribution/8e1c94d3-27dc-4d51-8de9-190dd50a471e>;
        dcat:theme              <http://datos.gob.es/kos/sector-publico/sector/medio-ambiente> , <http://publications.europa.eu/resource/authority/data-theme/ENVI> .

<http://data.europa.eu/88u/distribution/8e1c94d3-27dc-4d51-8de9-190dd50a471e>
        rdf:type        dcat:Distribution;
        dct:format      <https://datos.gob.es/catalogo/a12002994-datos-de-calidad-del-aire1/resource/a8fe5621-241f-4fad-9876-c87bb4d198d4/format>;
        dct:identifier  "https://abertos.xunta.gal/catalogo/medio-ambiente/-/dataset/0055/datos-calidade-aire/105/acceso-aos-datos.json"^^<http://www.w3.org/2001/XMLSchema#anyURI> ;
        dct:license     <https://creativecommons.org/licenses/by-sa/4.0/deed.gl>;
        dct:title       "Acceso aos datos"@gl, "Acceso a los datos"@es ;
        dct:description "La red de Calidad del Aire pone a disposición del publico la posibilidad de consultar la información actual del Índice de Calidad del Aire (ICA)."@es ;
        dcat:accessURL  <https://abertos.xunta.gal/catalogo/medio-ambiente/-/dataset/0055/datos-calidade-aire/105/acceso-aos-datos.json>;
        dcat:mediaType  <https://www.iana.org/assignments/media-types/application/json> ;
        dcat:service <http://datos.gob.es/dataservice/dataservice-ejemplo-1> ;
        dct:rights <http://datos.gob.es/catalogo/derechos-de-acceso> ;
        odrl:hasPolicy [ a odrl:Offer ;
                         odrl:permission [ odrl:action "publish" ;
                                           odrl:assigner <http://datos.gob.es/recurso/sector-publico/org/Organismo/A12002994> ] ] .

<http://data.europa.eu/88u/dataservice/6d284650-3c84-45f4-916e-4b9377e3555e>
  a dcat:DataService ;
  dct:title "Servicio del portal de Datos Abiertos de la Junta de Galicia"@es,  "Servizo de Portal de Datos Abertos da Xunta de Galicia"@gl ;
  dcat:endpointURL <https://abertos.xunta.gal/catalogo/> ;
  dct:publisher <http://datos.gob.es/recurso/sector-publico/org/Organismo/A12002994> ;
  dcatap:applicableLegislation <https://www.boe.es/eli/es-ga/l/2019/07/17/4/con> ;
  dcat:servesDataset <http://data.europa.eu/88u/dataset/0d24ea04-f026-4403-8df0-c9c6ff5174fd> .

<https://datos.gob.es/catalogo/a12002994-datos-de-calidad-del-aire1/resource/a8fe5621-241f-4fad-9876-c87bb4d198d4/format>
        rdf:type    dct:IMT;
        rdf:value   "application/json";
        rdfs:label  "JSON" .

<https://datos.gob.es/catalogo/a12002994-datos-de-calidad-del-aire1/Frequency>
        rdf:type   dct:Frequency;
        rdf:value  <https://datos.gob.es/catalogo/a12002994-datos-de-calidad-del-aire1/DurationDescription> .

<https://datos.gob.es/catalogo/a12002994-datos-de-calidad-del-aire1/DurationDescription>
        rdf:type   time:DurationDescription;
        time:days  "1"^^<http://www.w3.org/2001/XMLSchema#decimal> .

<http://publications.europa.eu/resource/authority/access-right/PUBLIC> a dct:RightsStatement .

<http://datos.gob.es/catalogo/derechos-de-acceso> a dct:RightsStatement ;
  rdfs:label "Derechos relativos a la reutilización del Catálogo de Datos Abiertos"@es .
```

Ilustración 12: ejemplo de conjunto de datos.

Las imágenes a continuación proporcionan ejemplos ilustrativos de interfaces gráficas del Catálogo de recursos, así como del detalle de una oferta:

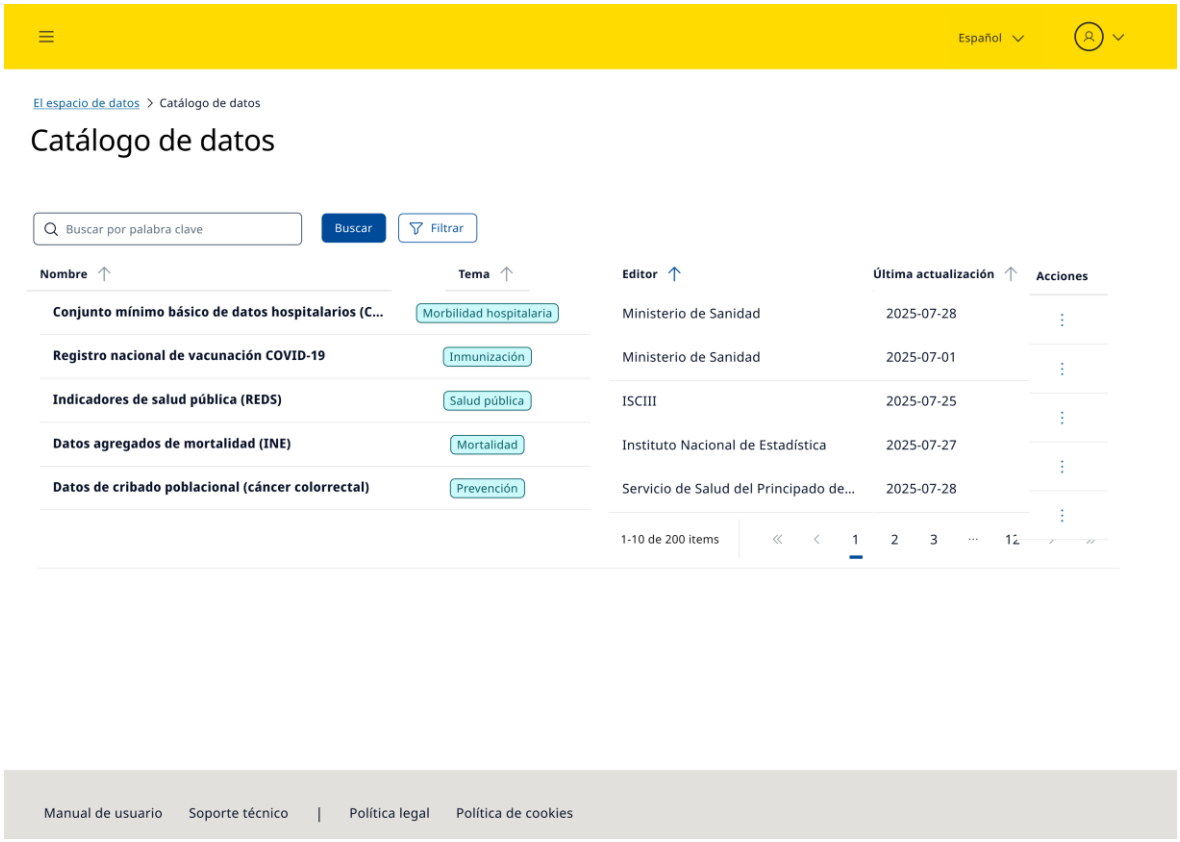


Ilustración 13: ejemplo de la interfaz gráfica del Catálogo de recursos.

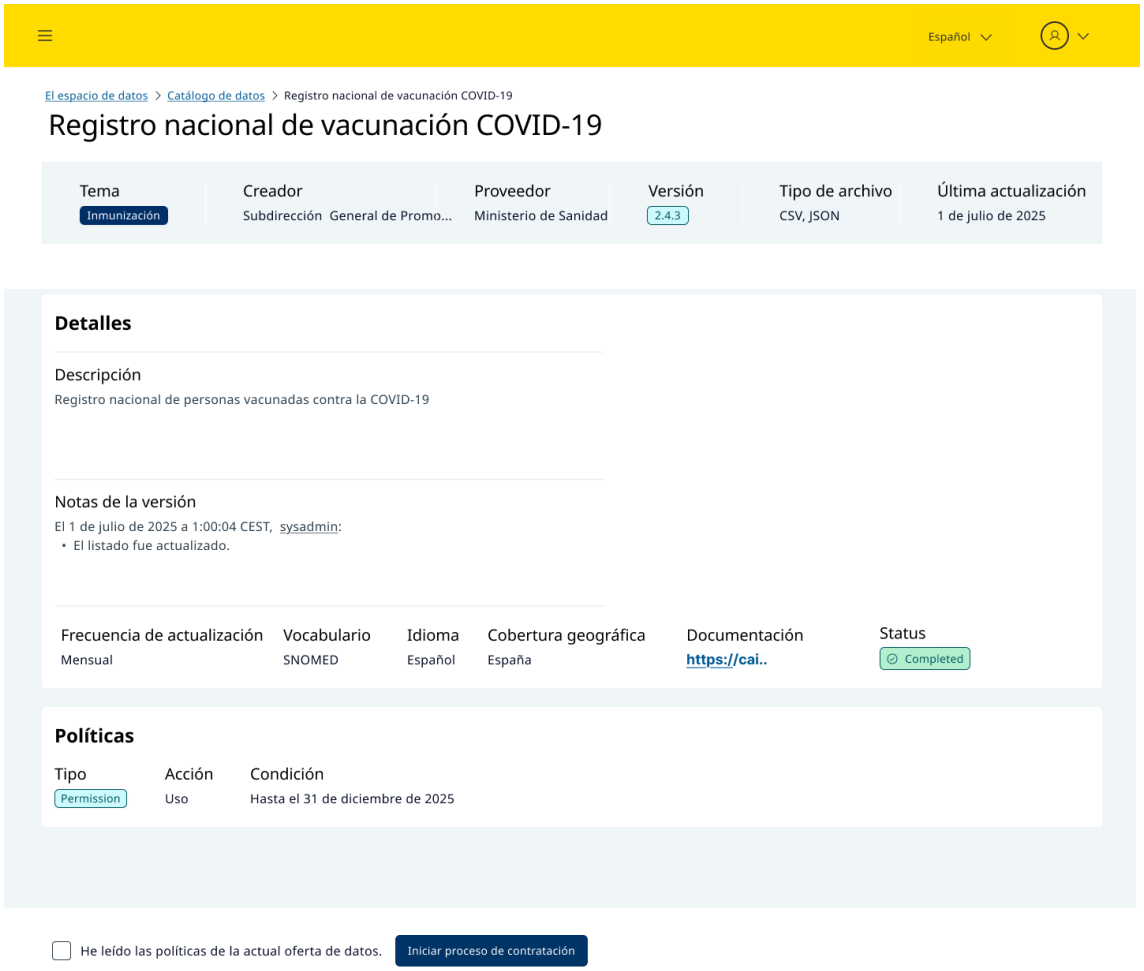


Ilustración 14: ejemplo de la interfaz gráfica del Catálogo de recursos. Dealle de una oferta.

4. Interacciones principales con otros componentes

El Catálogo se encuentra estrechamente vinculado con el resto del Marco Técnico:

- Identidad y Registro (3.2 y 3.3)
  - Permiten validar quién publica el activo.
  - Proveen información sobre roles y atributos del proveedor y consumidor.
- Biblioteca de vocabularios (3.5)
  - Suministra los vocabularios necesarios para la validación semántica.
  - Garantiza que los metadatos se describen con modelos compartidos.
- Motor de políticas (3.6)
  - Evalúa las políticas declaradas en el activo antes de la negociación.
  - Permite a los consumidores conocer restricciones y obligaciones.
- Conector (3.7)
  - Recupera las descripciones necesarias durante la negociación y transferencia.
  - Identifica métodos de acceso declarados en las distribuciones.

- Observabilidad (3.8)
  - Registra acciones sobre publicación, consulta o modificación de activo.
  - Permite reconstruir evidencias durante auditorías.

Estas interacciones convierten al catálogo en el eje semántico y operativo del espacio de datos.

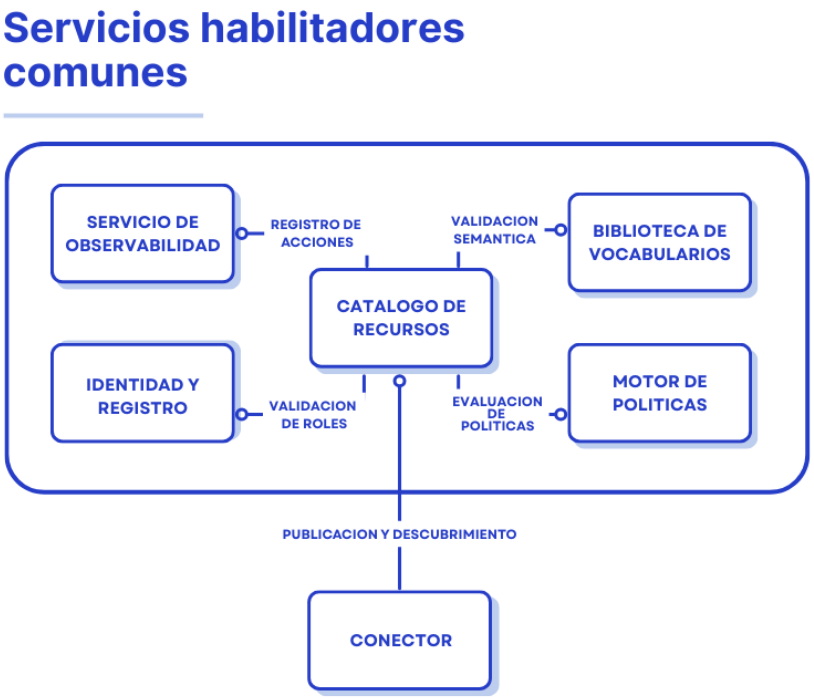


Ilustración 15: Interacciones del Catálogo de recursos

5. Aportación del componente a la interoperabilidad del ED

El catálogo es un habilitador crítico de interoperabilidad:

- Interoperabilidad legal
  - Asocia políticas de uso (ODRL) directamente al activo.
  - Permite conocer obligaciones, restricciones y finalidades antes de negociar.
- Interoperabilidad organizativa
  - Expone información del proveedor validada por el Registro.
  - Permite entender roles, responsabilidades y legitimaciones.
- Interoperabilidad semántica
  - Proporciona significado compartido mediante metadatos normalizados.
  - Aplica DCAT-AP, ODRL, DQV y PROV-O como base de interpretación común.
- Interoperabilidad técnica
  - Proporciona interfaces homogéneas de consulta y descubrimiento.

- Permite que cualquier conector pueda consumir las descripciones de los activos.

El catálogo es, por tanto, el punto de partida de todos los flujos operativos: sin un catálogo coherente, validado y estructurado, el espacio de datos no puede ofrecer ni descubrimiento, ni negociación, ni intercambio de datos de manera interoperable.

3.3.4. Biblioteca de vocabularios

La interoperabilidad en un espacio de datos no depende únicamente de la capacidad de intercambiar datos, sino también de la capacidad de interpretarlos de forma consistente entre organizaciones. Para ello es necesario que todos los participantes utilicen un conjunto común de vocabularios, modelos conceptuales y reglas semánticas que permitan describir los datos con un significado compartido. Esta base semántica es fundamental para garantizar la comprensión, comparación y reutilización de los activos publicados en el espacio de datos.

En este contexto, la Biblioteca de vocabularios actúa como el repositorio oficial del ecosistema, proporcionando los vocabularios, taxonomías y esquemas necesarios para validar y estructurar las descripciones que los proveedores publican en el Catálogo. Este componente asegura coherencia semántica en todos los procesos del espacio de datos - publicación, descubrimiento, evaluación, negociación y auditoría- y permite que el intercambio de datos sea realmente interoperable tanto dentro como entre espacios de datos.

1. **Descripción del componente**

Este componente debe considerarse como el catálogo de los vocabularios y especificaciones semánticas, incluyendo:

- Qué recursos semánticos se pueden encontrar.
- Quién ha publicado los recursos.
- Quién ha evolucionado los vocabularios
- Qué versiones existen.

2. **Funciones principales**

- Descubrimiento de recursos semánticos

La biblioteca debe permitir el descubrimiento de vocabularios y otros recursos semánticos para garantizar el entendimiento común.

- Publicación y mantenimiento de recursos semánticos

Este componente tiene que proporcionar los mecanismos para que los participantes puedan publicar los recursos semánticos necesarios, de la misma forma que pasa con el catálogo del espacio de datos.

- Reúso de recursos semánticos.

La biblioteca sirve como *hub* para después de la identificación permitir el acceso y reúso a los diferentes recursos semánticos publicados.

3. Servicios técnicos ofrecidos

Los componentes funcionales mínimos del Catálogo incluyen:

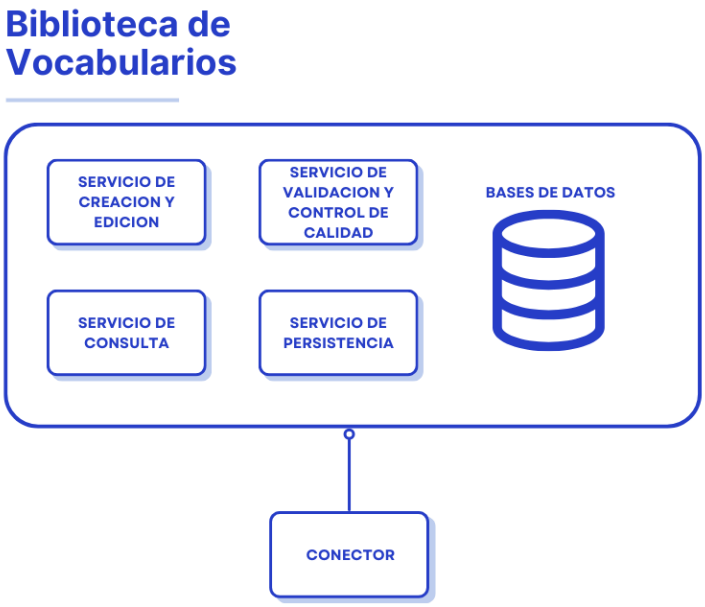


Ilustración 16: Componentes técnicos de la biblioteca de vocabularios

- Servicio de publicación y mantenimiento de los activos semánticos comunes.
- Servicio de validación y control de calidad de los activos semánticos comunes.
- Servicios de consulta del conjunto de vocabularios, ontologías, listas de códigos usadas en el contexto del ED.
- Servicio de persistencia.

De manera similar al Catálogo, la Biblioteca implementa DCAT-AP para su construcción. Para asegurar en todo momento la consistencia

El diagrama a continuación ofrece una visión a alto nivel de los modelos de datos en base a los que se estructuran los metadatos de la Biblioteca:

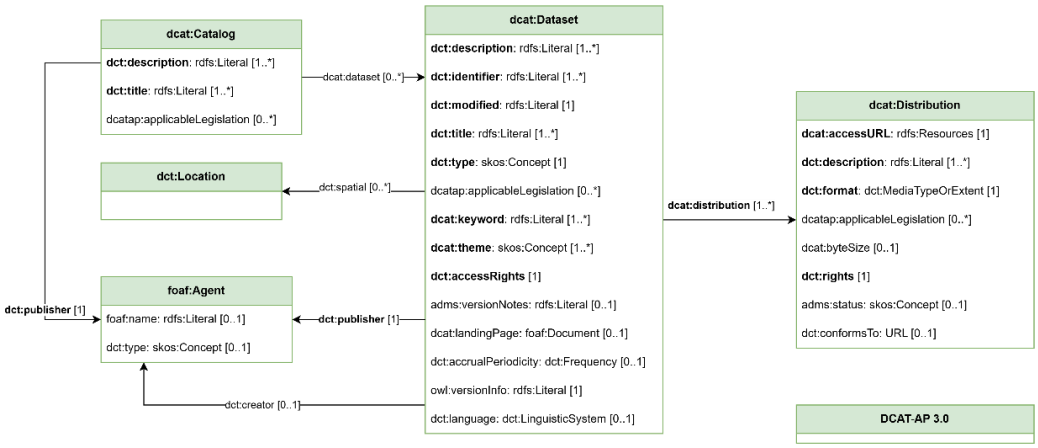
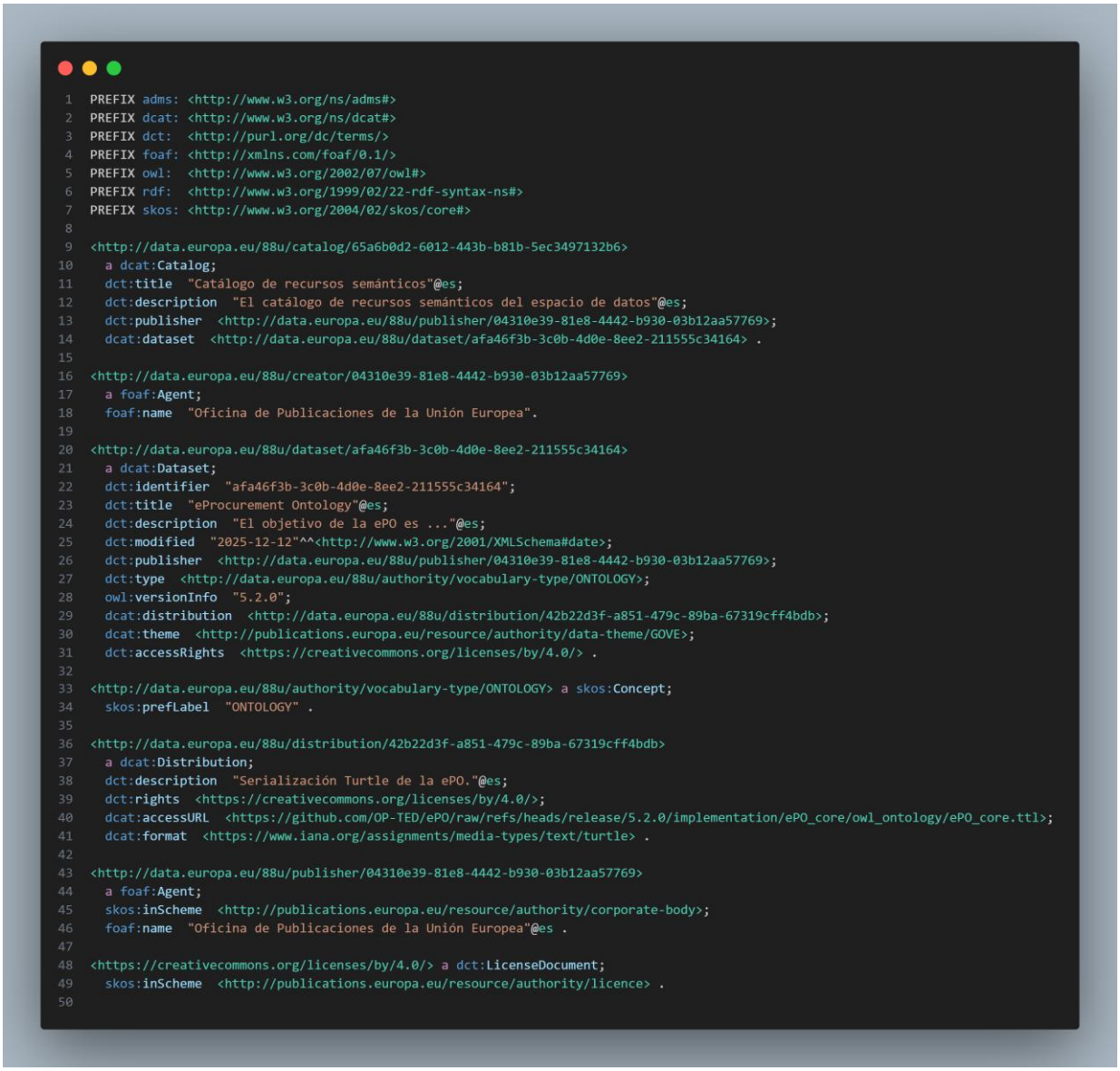


Ilustración 17: modelo de datos de la Biblioteca de vocabularios.

El código a continuación proporciona un ejemplo de vocabulario serializado en Turtle:



```
PREFIX adms: <http://www.w3.org/ns/adms#>
PREFIX dcat: <http://www.w3.org/ns/dcat#>
PREFIX dct:  <http://purl.org/dc/terms/>
PREFIX foaf: <http://xmlns.com/foaf/0.1/>
PREFIX owl:  <http://www.w3.org/2002/07/owl#>
PREFIX rdf:  <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX skos: <http://www.w3.org/2004/02/skos/core#>

<http://data.europa.eu/88u/catalog/65a6b0d2-6012-443b-b81b-5ec3497132b6>
  a dcat:Catalog;
  dct:title  "Catálogo de recursos semánticos"@es;
  dct:description  "El catálogo de recursos semánticos del espacio de datos"@es;
  dct:publisher  <http://data.europa.eu/88u/publisher/04310e39-81e8-4442-b930-03b12aa57769>;
  dcat:dataset  <http://data.europa.eu/88u/dataset/afa46f3b-3c0b-4d0e-8ee2-211555c34164> .

<http://data.europa.eu/88u/creator/04310e39-81e8-4442-b930-03b12aa57769>
  a foaf:Agent;
  foaf:name  "Oficina de Publicaciones de la Unión Europea".

<http://data.europa.eu/88u/dataset/afa46f3b-3c0b-4d0e-8ee2-211555c34164>
  a dcat:Dataset;
  dct:identifier  "afa46f3b-3c0b-4d0e-8ee2-211555c34164";
  dct:title  "eProcurement Ontology"@es;
  dct:description  "El objetivo de la ePO es ..."@es;
  dct:modified  "2025-12-12"^^<http://www.w3.org/2001/XMLSchema#date>;
  dct:publisher  <http://data.europa.eu/88u/publisher/04310e39-81e8-4442-b930-03b12aa57769>;
  dct:type  <http://data.europa.eu/88u/authority/vocabulary-type/ONTOLOGY>;
  owl:versionInfo  "5.2.0";
  dcat:distribution  <http://data.europa.eu/88u/distribution/42b22d3f-a851-479c-89ba-67319cff4bdb>;
  dcat:theme  <http://publications.europa.eu/resource/authority/data-theme/GOVE>;
  dct:accessRights  <https://creativecommons.org/licenses/by/4.0/> .

<http://data.europa.eu/88u/authority/vocabulary-type/ONTOLOGY> a skos:Concept;
  skos:prefLabel  "ONTOLOGY" .

<http://data.europa.eu/88u/distribution/42b22d3f-a851-479c-89ba-67319cff4bdb>
  a dcat:Distribution;
  dct:description  "Serialización Turtle de la ePO."@es;
  dct:rights  <https://creativecommons.org/licenses/by/4.0/>;
  dcat:accessURL  <https://github.com/OP-TED/ePO/raw/refs/heads/release/5.2.0/implementation/ePO_core/owl_ontology/ePO_core.ttl>;
  dcat:format  <https://www.iana.org/assignments/media-types/text/turtle> .

<http://data.europa.eu/88u/publisher/04310e39-81e8-4442-b930-03b12aa57769>
  a foaf:Agent;
  skos:inScheme  <http://publications.europa.eu/resource/authority/corporate-body>;
  foaf:name  "Oficina de Publicaciones de la Unión Europea"@es .

<https://creativecommons.org/licenses/by/4.0/> a dct:LicenseDocument;
  skos:inScheme  <http://publications.europa.eu/resource/authority/licence> .
```

Ilustración 18: ejemplo de serialización de una ontología.

La imagen a continuación ilustra una posible interfaz gráfica de la Biblioteca de vocabularios:

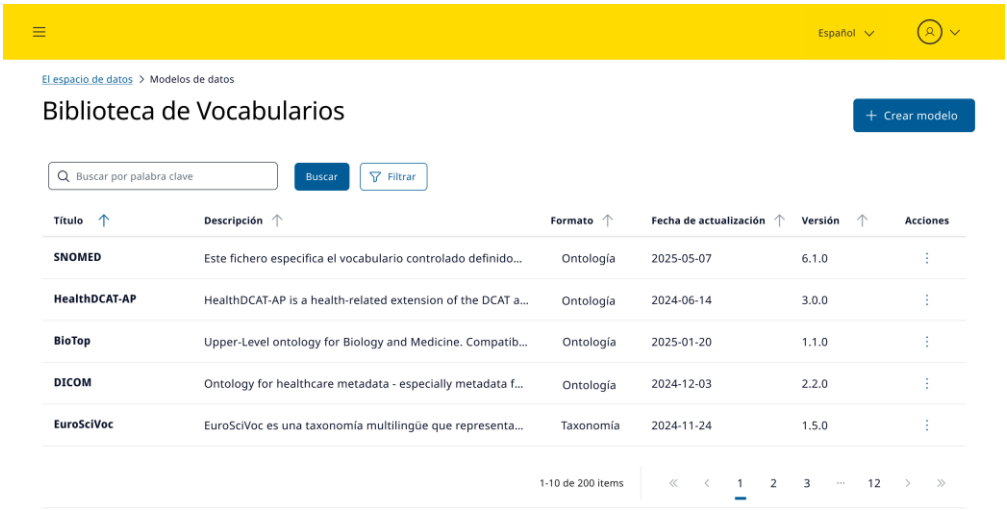


Ilustración 19; ejemplo de interfaz gráfica de la Biblioteca de vocabularios.

4. Interacciones principales con otros componentes

La biblioteca de vocabularios se vincula con otros componentes del Marco Técnico:

Ilustración 20: Interacciones principales de la biblioteca de vocabularios

- Identidad y Registro (3.2 y 3.3)
  - Permiten validar quién publica o modifica el recurso.
- Catálogo (3.4)
  - Incluye las descripciones de los conjuntos de datos usando las soluciones semánticas comunes.
- Conector (3.7)
  - Recupera las versiones y recursos semánticos usados en las descripciones de los conjuntos de datos relevantes para su descubrimiento y posterior explotación.
- Observabilidad (3.8)
  - Registra acciones sobre publicación, consulta o modificación de los diferentes recursos semánticos.
  - Permite reconstruir evidencias durante auditorías.

5. Aportación del componente a la interoperabilidad del ED

La biblioteca de vocabularios es un componente básico del espacio de datos y que tiene impacto a diferentes niveles:

- Interoperabilidad organizativa
  - Permite asegurar que los diferentes participantes trabajan bajo un marco común.
  - Proporciona la capacidad de trabajo coordinado y colaborativo en el desarrollo y mantenimiento de recursos semánticos.
- Interoperabilidad semántica
  - Permite y habilita la operación del espacio de datos y los participantes bajo un mismo marco semántico, asegurando la interoperabilidad mínima.
- Interoperabilidad técnica
  - Proporciona interfaces homogéneas de consulta y descubrimiento.
  - Permite que los conectores y servicios técnicos consuman las descripciones de una forma uniforme, favoreciendo la interoperabilidad técnica.

La biblioteca de vocabularios se constituye como una de las herramientas clave para garantizar la interoperabilidad semántica en los ED, permitiendo a los participantes compartir, gestionar y enriquecer los distintos artefactos semánticos, vocabularios controlados, ontologías y artefactos necesarios para garantizar el correcto uso estándar de términos para describir los datos que proveen o consumen.

3.3.5. Motor de políticas

El intercambio gobernado de datos en un espacio de datos requiere que las condiciones de acceso y uso se apliquen de forma automática, consistente y verificable. Para ello, el Marco Técnico debe contar con un componente especializado capaz de interpretar y ejecutar las políticas definidas por los proveedores, asegurando que cada interacción – desde la negociación hasta la transferencia y el uso posterior – cumple estrictamente con lo establecido en el Marco de Gobernanza y en los contratos específicos. La UNE

0087:2025 destaca que la interoperabilidad sólo puede garantizarse si las reglas del ecosistema pueden evaluarse de manera determinista y sin ambigüedades.

1. **Descripción del componente**

El Motor de Políticas es el componente responsable de interpretar, evaluar y aplicar automáticamente las condiciones de acceso y uso asociadas a los activos publicados en el espacio de datos. Estas condiciones se expresan mediante políticas legibles por máquina, que definen permisos, prohibiciones, obligaciones y restricciones que deben cumplirse tanto en la fase de negociación como en la transferencia y el uso posterior del dato.

La existencia de este componente permite trasladar el Marco de Gobernanza al plano técnico, garantizando que los datos solo se utilizan bajo las condiciones acordadas y que las decisiones de autorización se aplican de forma coherente y verificable por todos los participantes.

2. **Funciones principales**

1. Interpretación de políticas declaradas en los activos

El motor debe ser capaz de interpretar las políticas asociadas a cada activo -habitualmente expresadas en ODRL- incluyendo permisos, prohibiciones, obligaciones, restricciones contextuales, finalidades o limitaciones temporales.

2. Evaluación de condiciones de uso durante la negociación

Permite determinar si un consumidor puede acceder a un activo según:

- Su identidad.
- Sus atributos verificados.
- Su rol dentro del espacio de datos.
- La finalidad declarada.
- Las restricciones del activo.

Este proceso es previo a la formalización del contrato.

3. Generación de resultados de autorización

Tras evaluar una política, el componente produce un resultado determinista que indica:

- Autorización.
- Denegación.
- Autorización condicionada
- Solicitud de información adicional.

4. Soporte a la transferencia gobernada

Durante la transferencia, el motor puede verificar si:

- El uso es conforme al contrato.
- Se respetan límites temporales o de volumen.
- Se mantiene la finalidad acordada.
- Existen obligaciones posteriores (ej. Borrado o retención.)

5. Auditoría del cumplimiento de políticas.

El motor genera información que permite reconstruir qué políticas se evaluaron, con qué criterios y qué decisiones se tomaron, facilitando auditorías posteriores.

3. Servicios técnicos ofrecidos

El motor de Políticas suele ofrecer, como mínimo, los siguientes servicios técnicos accesibles mediante API:

Ilustración 21: Componentes fundamentales del motor de políticas

- Servicio de evaluación de políticas. Evalúa un conjunto de políticas asociadas a un activo frente a los atributos del consumidor, el contexto y la solicitud.
- Servicio de interpretación de reglas. Permite a componentes como el Catálogo o el Conector obtener una representación procesable de la política.
- Servicio de autorización. Produce una decisión formal de acceso, incluyendo información sobre obligaciones y restricciones aplicables.
- Servicio de validación de políticas. Comprueba que las políticas declaradas por un proveedor están correctamente estructuradas, son coherentes y utilizables dentro del modelo semántico del ED.
- Servicio de resolución de conflictos. Gestiona casos en los que múltiples políticas aplican simultáneamente o entran en conflicto.
- Servicio de auditoría. Permite consultar los resultados de evaluaciones previas para fines de supervisión, trazabilidad o certificación.

Las políticas deben ser definidas siguiendo el estándar de ODRL. El diagrama a continuación muestra el modelo de datos de éstas

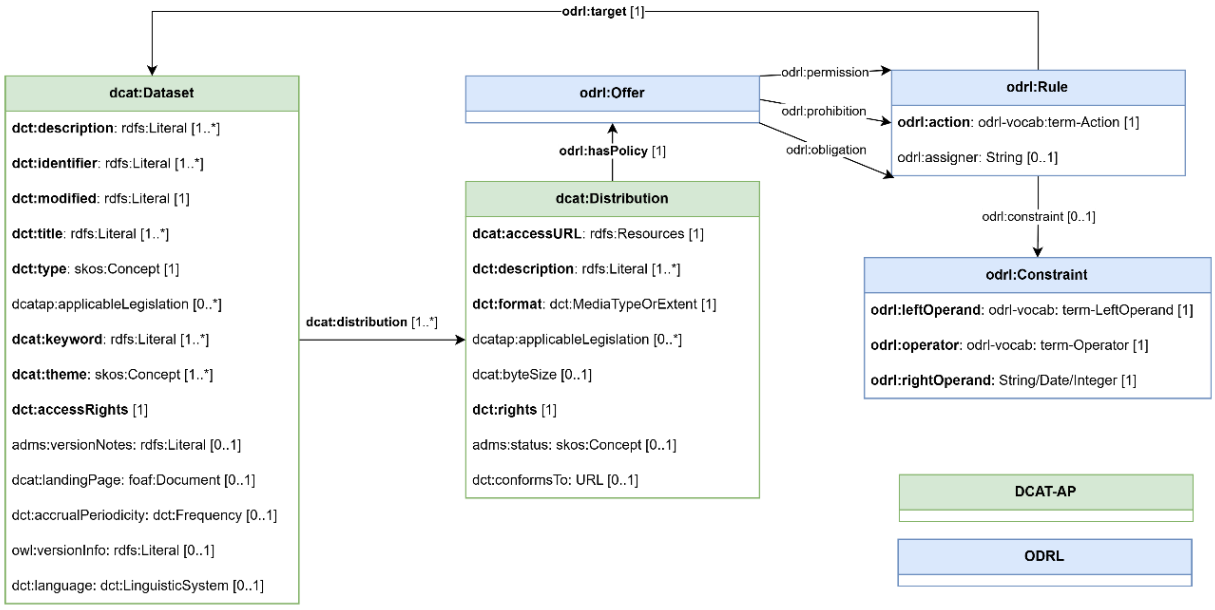


Ilustración 22: modelo de datos de las políticas.

La imagen a continuación presenta un ejemplo de documento ODRL de una oferta serializado en Turtle:

```
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#> .
PREFIX odrl: <http://www.w3.org/ns/odrl/2/>


<http://data.europa.eu/88u/offer/1706bbb6-e4b0-4ce3-a1b0-07836f2f6740> a odrl:Offer ;
    odrl:uid "1706bbb6-e4b0-4ce3-a1b0-07836f2f6740"^^xsd:string ;
    odrl:permission [
        odrl:target <http://data.europa.eu/88u/dataset/0d24ea04-f026-4403-8df0-c9c6ff5174fd> ;
        odrl:assigner  <http://datos.gob.es/recurso/sector-publico/org/Organismo/A12002994> ;
        odrl:action odrl:use ;
        odrl:constraint [
            odrl:leftOperand odrl:spatial ;
            odrl:operator odrl:eq;
            odrl:rightOperandReference <https://publications.europa.eu/resource/authority/country/ESP> ;
        ]
    ] .
```

Ilustración 23: ejemplo de documento ODR de una oferta.

4. Interacciones principales con otros componentes

El Motor de Políticas interactúa intensamente con el resto de los componentes del Marco Técnico:

Ilustración 24: Interacciones principales del motor de políticas

- Identidad y Registro (3.2 y 3.3)
  - El motor utiliza atributos verificados del participante para evaluar si cumple las condiciones de acceso.
- Catálogo de Recursos (3.4)
  - Consume las políticas asociadas a cada activo para interpretarlas y prepararlas para una posterior negociación.
- Biblioteca de vocabularios (3.5)
  - Necesita vocabularios comunes para interpretar correctamente términos utilizados en políticas (roles, acciones, categorías, condiciones).
- Conector (3.7)
  - Es el componente que invoca las evaluaciones durante la negociación y antes/durante la transferencia.
  - Aplica las decisiones (permitido / denegado / condicionado).
- Observabilidad (3.8)
  - Registra evidencia de todas las decisiones de autorización.
  - Permite reconstruir el razonamiento y las políticas aplicadas.

El Motor de Políticas interviene en momentos clave: evaluación inicial, verificación en tiempo real, aplicación de obligaciones y soporte post-uso.

5. Aportación del componente a la interoperabilidad del ED

El Motor de Políticas garantiza que las reglas del espacio de datos se aplican de forma uniforme, automática y verificable, contribuyendo a todas las dimensiones de interoperabilidad:

- Interoperabilidad legal
  - Transforma reglas y condiciones legales en políticas técnicas evaluables.
  - Garantiza que el uso del dato se ajusta a las condiciones acordadas.
- Interoperabilidad organizativa
  - Permite que roles y obligaciones del Marco de Gobernanza se trasladen a la operación técnica.
- Interoperabilidad semántica
  - Aplica vocabularios comunes para interpretar cláusulas de permisos, prohibiciones u obligaciones.
- Interoperabilidad técnica
  - Proporciona evaluaciones deterministas y consistentes, independientemente del proveedor o consumidor.

En síntesis, el Motor de Políticas es el mecanismo que asegura que todo intercambio de datos se ajusta a las reglas del espacio de datos y que dichas reglas se aplican de forma coherente en cada interacción.

3.3.6. Conector

El conector es el componente técnico que hace posible la interacción directa entre los participantes de un espacio de datos. Su función es ejecutar, de forma automatizada y segura, los procesos de negociación, autorización y transferencia definidos por el Marco de Gobernanza y soportados por el Marco Técnico.

En la práctica, el conector actúa como el punto de entrada y salida del espacio de datos para cada organización: es el componente que representa técnicamente al participante ante el ecosistema y que aplica las políticas, identidades, atributos y decisiones de autorización durante todo el ciclo operativo.

En la UNE 0087:2025 se dice que, sin un conector interoperable, ningún espacio de datos puede garantizar un intercambio gobernado, trazable ni reproducible. Por ello, el conector constituye uno de los elementos centrales del Marco Técnico.

1. **Descripción del componente**

El conector es el componente software que habilita la comunicación entre un participante y el resto del espacio de datos mediante:

- autenticación y autorización basadas en identidades verificables,
- interpretación y aplicación de políticas,
- negociación de condiciones de uso,
- transferencia segura de datos,
- generación de evidencias verificables,
- y cumplimiento de obligaciones contractuales durante y después del intercambio.

El conector no sustituye los sistemas internos de las organizaciones, sino que actúa como una pasarela gobernada, que garantiza:

- que las solicitudes salientes cumplen las políticas del proveedor,
- que las solicitudes entrantes cumplen los requisitos del consumidor,

- y que ninguna interacción se produce fuera de las reglas del espacio de datos.

El conector implementa una arquitectura en dos planos:

- Plano de control

Gestiona autenticación, evaluación de políticas, negociación y emisiones de decisiones.

- Plano de datos

Gestiona la transferencia segura, el cumplimiento del contrato y la trazabilidad técnica.

2. Funciones principales

1. Autenticación mutua y validación de credenciales

El conector valida las identidades y atributos de la contraparte utilizando las credenciales verificables emitidas en el espacio de datos.

2. Negociación de condiciones de uso

Intercambia solicitudes, ofertas y respuestas conforme a las políticas declaradas en el Catálogo y evaluadas por el Motor de Políticas.

3. Evaluación y aplicación de políticas

El conector aplica las decisiones del Motor de Políticas, garantizando que:

- solo se autoriza lo permitido,
- se rechaza lo prohibido,
- y se aplican obligaciones u operaciones necesarias (filtros, anonimización, restricciones...).

4. Transferencia segura de datos

Gestiona canales cifrados y mecanismos de transporte (push/pull/streaming), controlando el flujo conforme al contrato.

5. Generación de evidencias técnicas

Produce eventos verificables para auditoría: identidad usada, política evaluada, activo solicitado, parámetros de transferencia, estado final.

6. Gestión de cancelaciones e incidencias

Interrumpe o invalida una transferencia si detecta incumplimiento o error técnico, registrando motivos y evidencia.

3. Servicios técnicos ofrecidos

El conector ofrece servicios expuestos mediante APIs internas y externas:

Ilustración 25: Componentes fundamentales del conector

- Servicio de autenticación y autorización.
  - Verifica identidades y atributos
  - Emite decisiones de autorización basadas en políticas
- Servicio de negociación
  - Intercambia mensajes de solicitud, oferta y aceptación
  - Produce el contrato técnico que habilita la transferencia
- Servicio de transferencia
  - Establece canales seguros
  - Gestiona mecanismos de intercambio (pull/push/stream)
  - Aplica restricciones y obligaciones
- Servicio de evidencias y auditoría
  - Genera eventos estructurados
  - Expone trazas para supervisión y certificación
- Servicio de cumplimiento de políticas
  - Aplica reglas en tiempo real durante el tránsito del dato
- Servicio de conexión con sistemas internos
  - Permite integrar los datos internos del participante con el conector sin comprometer soberanía ni seguridad.

Estos servicios permiten que cualquier participante del espacio de datos implemente un conector conforme a las reglas del Marco Técnico.

4. Interacciones principales con otros componentes

Ilustración 26: Interacciones principales del conector

- Identidad y Registro (3.2 y 3.3)
  - El conector utiliza identidades verificables y atributos certificados en todos los flujos.
  - Solo interactúa con participantes activos y autorizados.
- Catálogo (3.4)
  - Recupera todos los metadatos necesarios para negociar acceso:
  - políticas, calidad, condiciones de uso, información técnica del activo.
- Biblioteca de vocabularios (3.5)
  - Garantiza que el conector interpreta adecuadamente los términos semánticos usados en catálogos y políticas.
- Motor de Políticas (3.6)
  - Invoca y aplica decisiones de autorización durante negociación y transferencia.
- Observabilidad y Auditoría (3.8)
  Registra cada acción crítica:
  - evaluación de políticas,
  - identidades utilizadas,
  - inicio y fin de transferencia,
  - incumplimientos,

- evidencias criptográficas.

Estas interacciones hacen del conector el componente más integrado del Marco Técnico.

5. **Aportación del componente a la interoperabilidad del ED**

El conector hace posible la interoperabilidad técnica efectiva del espacio de datos:

- Interoperabilidad legal. Aplica automáticamente las condiciones contractuales acordadas.
- Interoperabilidad organizativa. Respeta roles, atributos y legitimaciones establecidas por la gobernanza.
- Interoperabilidad semántica. Interpreta políticas y metadatos conforme a vocabularios comunes.
- Interoperabilidad técnica. Ejecuta procesos compatibles entre organizaciones heterogéneas.

Sin un conector interoperable y gobernado:

- no hay negociación,
- no hay transferencia segura,
- no hay trazabilidad suficiente,
- y no hay soberanía técnica del dato.

El conector es, por tanto, el habilitador operativo central del espacio de datos.

Este modelo de conector es coherente con las especificaciones del Dataspace Protocol (DSP) y con implementaciones de referencia como Eclipse Dataspace Components (EDC), utilizadas en el contexto de iniciativas europeas como SIMPL-Open

3.3.7. Servicio de Observabilidad

La Observabilidad y la Auditoría Técnica constituyen el componente responsable de registrar, correlacionar y poner a disposición todas las evidencias necesarias para asegurar que las interacciones del espacio de datos se ejecutan de forma transparente, verificable y conforme al Marco de Gobernanza.

Según la UNE 0087:2025, la interoperabilidad técnica requiere que cada intercambio pueda ser reconstruido en base a evidencias objetivas, incluyendo:

- quién actuó,
- qué solicitó,
- qué políticas se evaluaron,
- qué decisiones se tomaron,
- cómo se realizó la transferencia,
- y cuál fue el resultado final.

Este componente es fundamental no solo para auditorías internas o externas, sino también para verificar la conformidad y la interoperabilidad de los conectores y servicios habilitadores del ecosistema.

1. **Descripción del componente**

El componente de Observabilidad y Auditoría Técnica recopila y gestiona los eventos y evidencias generados durante el ciclo de vida de todas las interacciones del espacio de datos.

Esto incluye eventos relativos a:

- identidad y autenticación,
- consultas al catálogo,
- evaluaciones de políticas,
- procesos de negociación,
- transferencias de datos,
- estados finales del intercambio,
- y obligaciones posteriores al uso.

Este componente no evalúa políticas ni autoriza accesos, sino que registra de forma estructurada y verificable todo lo que ocurre, proporcionando información para:

- auditoría,
- supervisión,
- resolución de disputas,
- certificación,
- y mejora continua.

La observabilidad garantiza transparencia dentro del ED, mientras que la auditoría garantiza responsabilidad.

2. Funciones principales

1. Recopilación de eventos técnicos

Registra eventos emitidos por conectores, motor de políticas, identidad, catálogo y otros servicios habilitadores.

2. Generación de evidencias verificables

Produce evidencias estructuradas que permitan demostrar el cumplimiento de políticas y contratos.

3. Correlación de eventos

Permite reconstruir líneas de tiempo de procesos completos (publicación, negociación, transferencia...).

4. Soporte para auditoría interna y externa

Ofrece información consistente para verificar cumplimiento técnico, contractual y operativo.

5. Conservación y retención conforme a políticas

Gestiona la retención de evidencias según las normas del espacio de datos o la regulación aplicable.

3. Servicios técnicos ofrecidos

El componente expone al menos los siguientes servicios:

Ilustración 27: Componentes fundamentales del servicio de observabilidad

- Servicio de registro de eventos. Permite a otros componentes enviar eventos estructurados (JSON-LD, RDF u otro formato común).
- Servicio de consulta de evidencias. Recupera eventos asociados a una operación, recurso, contrato o participante.
- Servicio de correlación. Reconstruye secuencias completas de interacción.
- Servicio de auditoría. Expone información relevante para verificaciones periódicas o certificación.
- Servicio de exportación. Permite transferir evidencias a herramientas externas.
- Servicio de gestión de retención. Controla tiempos de retención de evidencias y aplica borrados condicionados.

El código a continuación ilustra el registro de un evento (transferencia):

```
{
  "transfer_id": "8ad692dc-c50e-43c2-babc-d547a8be8ad9",
  "created": "2024-06-10T15:30:00.123Z",
  "availability_date": "2024-06-10T15:31:00.123Z",
  "transfer_type": "HttpData-PULL",
  "status": "TERMINATED",
  "protocol": "dataspace-protocol-http",
  "dataset_id": "0d24ea04-f026-4403-8df0-c9c6ff5174fd",
  "resource_title": "Datos de calidad del aire",
  "contract_id": "1ad692dc-c56e-45c2-babc-d547a8be8ad9",
  "connector_provider_id": "7ad692dc-c56e-45c2-bcbl-d547a8be8ad9",
  "connector_consumer_id": "1ad692dc-c58e-45c2-babc-d547a8be8ad9",
    "user_id": "1ddsfdsdc-c56e-45c2-babc-d547a8be8ad9"
}
```

Ilustración 28: ejemplo de un registro de transferencia.

4. Interacciones principales con otros componentes

Ilustración 29: Interacciones principales entre componentes

- Identidad y Registro (3.2 y 3.3)
  - Registra validaciones de credenciales, atributos utilizados y estado del participante.
- Catálogo (3.4)
  - Registra publicación, edición, retirada y consultas de activos.
- Biblioteca de vocabularios (3.5)
  - Genera evidencias relativas a validaciones semánticas.
- Motor de Políticas (3.6)
  - Registra evaluaciones de permisos, prohibiciones, obligaciones y decisiones resultantes.
- Conector (3.7)
  - Registra eventos clave del plano de control y del plano de datos: autenticación, negociación, transferencia, interrupciones, errores, resultados finales.

5. Aportación del componente a la interoperabilidad del ED

- Interoperabilidad legal.
  - Permite demostrar cumplimiento de contratos y políticas.
  - Garantiza responsabilidad y trazabilidad jurídica.
- Interoperabilidad organizativa
  - Facilita supervisión continua y resolución de incidencias.
  - Aporta transparencia y confianza al ecosistema.
- Interoperabilidad semántica
  - Registra validaciones semánticas y metadatos asociados al linaje (PROV-O).
- Interoperabilidad técnica
  - Permite reconstruir qué ocurrió en un intercambio.
  - Asegura coherencia, trazabilidad y verificación entre implementaciones diferentes.

En conjunto, la Observabilidad y Auditoría Técnica es el mecanismo que garantiza la confianza operativa del espacio de datos, permitiendo que el ecosistema funcione con seguridad, responsabilidad y transparencia.

3.4. Interoperabilidad semántica y sintáctica

La interoperabilidad semántica y sintáctica constituye un aspecto clave a implementar para asegurar la cadena de valor compuesta por un correcto modelado, descripción, intercambio, comprensión, reutilización y posterior generación de valor a partir de los datos.

En los espacios de datos describimos estas capacidades semánticas a través de dos pilares fundamentales; la interoperabilidad semántica base, aquella que debe ser implementada de manera transversal y presente en todos los servicios habilitadores y componentes, y la interoperabilidad semántica sectorial o de dominio.

El presente documento da cobertura principalmente al primer pilar, describiendo como cada componente, servicio y operación hace uso de distintos modelos y formatos normalizados para garantizar la correcta descripción y serialización de metadatos y atributos relativos a los datos. A modo de recapitulación, se relacionan los siguientes modelos y estructuras normalizadas indicadas para dicho propósito:

- DCAT-AP: como perfil obligatorio para describir conjuntos de datos, distribuciones y servicios de datos. Este perfil es el desarrollado y recomendado por la Comisión Europea para la interoperabilidad de catálogos públicos de datos. Dicho perfil podrá, a su vez, ser extendido según las necesidades específicas del espacio de datos.
- RDF y JSON-LD: como formatos estructurados para la representación de metadatos.
- PROV-O: para la descripción del linaje del dato.
- DQV: para la representación de métricas de calidad.
- ODRL: para la representación de políticas y contratos.
- SHACL: para la validación formal de esquemas y estructuras.

Por otro lado, entendemos la interoperabilidad semántica sectorial como la capacidad de que diferentes organizaciones dentro del mismo sector modelen, describan e intercambien datos compartiendo un significado común, aspecto fundamental para permitir su posterior reutilización y extracción de valor. En este ámbito existen diversas iniciativas y múltiples posibilidades para gestionar los datos sectoriales, desarrolladas de manera asimétrica dentro de distintos dominios a lo largo de los últimos años.

El presente documento no profundiza en este aspecto, sin embargo, dentro de la Hoja de Ruta del Marco de Referencia Técnico del Centro de Referencia de Espacios de Datos, y en colaboración con UNE y el Subcomité 43, se ha comenzado con la formación de grupos de trabajo específicos que abordarán esta misión de manera sectorial, con el objetivo de analizar el estado del arte en los distintos sectores priorizados, y elaborar colecciones y recomendaciones sobre los artefactos semánticos disponibles y utilizables para distintos propósitos, así como identificar las distintas necesidades adicionales en el ámbito de la generación y normalización de modelos de datos interoperables.

3.5. Tecnologías para la implementación de espacios de datos

Las decisiones tecnológicas, más allá del diseño de la arquitectura correspondiente, constituyen un elemento fundamental a la hora de diseñar e implementar un espacio de datos. Dichas decisiones constituyen a menudo una gran dificultad para los promotores de los espacios de datos. Con el propósito de facilitar la toma de decisiones en este sentido, bien orientada al propio desarrollo de la tecnología o a la compra de estas capacidades técnicas a un tercero, se relacionan, de manera no exhaustiva, un listado de tecnologías recomendadas.

Los **criterios generales** a la hora de seleccionar el conjunto de tecnologías elegidas deben ser en cualquier caso los siguientes:

- **Adecuación al caso de uso:** La tecnología debe resolver claramente la necesidad funcional, y ser justificada adecuadamente a partir de dichos propósitos.
- **Madurez y estabilidad:** Se deben tener en cuenta aspectos fundamentales como su nivel TRL, versiones estables, frecuencia de *releases* y uso probado en entornos productivos y casos de uso reales.
- **Comunidad, soporte y ecosistema:** Disponibilidad de soporte profesional, existencia de comunidad activa, capacidades de integración con otras herramientas.
- **Coste total de propiedad:** Costes de licencias, operación y mantenimiento, recursos necesarios, costes de escalado y costes de migración futura.
- **Riesgo de dependencia:** Preferencia por estándares abiertos y APIs compatibles, modelos de datos exportables y no propietarios.
- **Interoperabilidad y estándares:** Cumplimiento de protocolos, formatos de datos estándar, capacidad para integrarse en arquitecturas híbridas y *multicloud*, aceptación de la industria.
- **Seguridad y cumplimiento regulatorio:** Soporte para cifrado, autenticación, autorización y auditoría, cumplimiento de normativas GDPR y sectoriales.
- **Escalabilidad y rendimiento:** Demostrada en entornos reales, escalado horizontal nativo como preferencia, uso eficiente de recursos y compatibilidad con arquitecturas distribuidas (Kubernetes, serverless...)
- **Observabilidad y operatividad:** Métricas, logs estructurados y trazabilidad distribuida, integración con herramientas de observabilidad y monitorización (Prometheus, Grafana ELK...), facilidad de despliegue y automatización.
- **Alineamiento con la estrategia tecnológica corporativa:** Consistencia con el ecosistema tecnológico actual, reutilización de capacidades y competencias disponibles en la organización.

De la misma manera, se aportan indicaciones sobre **buenas prácticas** a la hora de seleccionar tecnologías:

- **Evaluar mediante pruebas de concepto:** Validación de rendimiento, integración y escalabilidad utilizando casos de uso reales, evitar decisiones solo teóricas o basadas en documentación.
- **Comparación objetiva con criterios ponderados:** Generación de matrices de decisión con criterios de negocio, técnicos y operativos.
- **Adoptar el principio "menos es más":** Evitar la "sobretecnificación", preferir tecnologías que simplifiquen la arquitectura, reducir el número de *stacks* compatibles.
- **Priorizar estándares abiertos y tecnologías ampliamente adoptadas:** Minimizar el "vendor lock-in" y facilitar encontrar talento capacitado para el desarrollo y mantenimiento, mayores garantías de soporte a largo plazo.
- **Asegurar coherencia entre componentes:** Verificar compatibilidad entre herramientas del *stack*, revisar patrones de integración y considerar el ciclo de vida completo.
- **Evitar el impacto en la gobernanza de datos:** Asegurar compatibilidad con catálogo, linaje, calidad y políticas.

- **Revisar escenarios de escalado y resiliencia:** Pruebas de estrés, plan de continuidad, *backup* y recuperación, comportamiento ante fallos de red o picos de carga.
- **Planificar la evolución y deprecación:** Elegir tecnologías que tengan un plan de desarrollo claro, establecer criterios para su sustitución futura, evitar *stacks* sin mantenimiento o con señales de obsolescencia.

Relación no exhaustiva de tecnologías para la implementación, estructuradas por capas dentro del *stack*:

Capa	Tecnologías y estándares relevantes
Ingesta de datos	• Apache Kafka • Apache NiFi • Apache Pulsar
Almacenamiento y persistencia	• PostgreSQL/ MySQL/MariaDB • MongoDB/Opensearch/Elasticsearch • Redis • GraphDB • Neo4j • Apache Jena Fuseki
Procesamiento y transformación	• Apache Spark • Apache Flink • Apache Beam • Apache Airflow • Kafka Streams
Semántica y gobierno del dato	• RDF • RDFS • OWL • SHACL • SKOS • ODRL (políticas de uso) • DCAT / DCAT-AP • IDS Information Model • Apache Atlas • OpenMetadata
Seguridad, identidad y control de acceso	• Keycloak • OAuth 2.0 • OpenID Connect • X.509 / PKI

Capa	Tecnologías y estándares relevantes
	• W3C Verifiable Credentials • DID • AuthzForce
Observabilidad	• ELK: Elasticsearch, Logstash, Kibana • Prometheus + Grafana • Registros de auditoría basados en Blockchain
Exposición y consumo de datos	• API Gateways • Kong • WSO2 • Traefik • GraphQL • Apache Superset
Infraestructura y operación	• Kubernetes • Helm • Terraform • Ansible • Prometheus • Grafana

Tabla 1: relación de tecnologías para la implementación de espacios de datos.

Además de las tecnologías anteriormente mencionadas, para la implementación de los componentes del *stack* orientados a habilitar especialmente la interoperabilidad entre espacios de datos, existen numerosas iniciativas a nivel nacional e internacional que se encuentran desarrollando soluciones innovadoras, y cuyo grado de madurez varía, sin estar ninguna de ellas ampliamente adoptadas en sistemas productivos a día de hoy, se aporta una relación compuesta de distintos artefactos tales como especificaciones, servicios, protocolos o componentes técnicos:

- Eclipse Dataspace Components (EDC).
- Dataspace Protocol (DSP).
- FIWARE Data Space Connector.
- Gaia-X Trust Framework & Digital Clearing House
- SIMPL-Open

3.6. Interoperabilidad dentro y entre espacios de datos

El propósito de esta sección es el de describir y guiar en los procesos y operaciones fundamentales que deben ser implementados para conseguir la interoperabilidad en espacios de datos. Esta se puede ver y conseguir por fases o etapas, en una primera

instancia: **dentro de un espacio de datos**, es decir, la interoperabilidad entre sus participantes y servicios. De esta manera, los proyectos priorizan la puesta en marcha efectiva de sus casos de uso, incorporación de participantes y datos, enfocándose en la generación de valor y retorno de la inversión. Posteriormente, existe una segunda etapa donde la interoperabilidad se establece **entre varios ecosistemas de compartición de datos**, para que así puedan, si sus objetivos o negocio así lo necesitaran, de manera conjunta, generar valor a partir de casos de uso conjuntos habilitados mediante el intercambio y extracción de valor de los datos.

A continuación, se definen procesos y capacidades necesarios para ambas etapas, con un foco más profundo en dar soporte a la primera, el establecimiento de un espacio de datos maduro e interoperable. El enfoque se centra en promover la creación de valor a partir de los datos, asegurando el retorno para los participantes y su negocio y objetivos, así como la consecución de los casos de uso, poniendo el foco en entornos maduros basados en estándares abiertos que permitan una posterior interoperabilidad con otros ecosistemas.

3.6.1. Cómo interoperar dentro del espacio de datos

Una vez definidos los componentes esenciales del Marco de Interoperabilidad Técnico, es necesario comprender **cómo interactúan entre sí para habilitar el funcionamiento real del espacio de datos.** Los componentes no operan de manera aislada: su propósito es desplegar, de forma coordinada, los procesos que permiten a los participantes publicar datos, descubrir activos, negociar condiciones de uso, intercambiar información de manera segura y generar evidencias verificables durante todo el ciclo de vida del dato.

Estos procesos técnicos constituyen la columna vertebral operativa del espacio de datos. Representan la forma en que los principios del Marco de Gobernanza y las capacidades del Marco Técnico se convierten en acciones concretas ejecutadas por los conectores y servicios habilitadores. Su diseño debe ser homogéneo, repetible y neutral tecnológicamente, de modo que cualquier organización pueda integrarse en el ecosistema aplicando el mismo conjunto de reglas y mecanismos comunes.

3.6.1.1. Adhesión

La adhesión es el proceso mediante el cual una entidad adquiere la condición de participante autorizado del espacio de datos. Este flujo operativo garantiza que solo organizaciones legítimas, identificadas de manera verificable y aceptadas por la autoridad de gobernanza, puedan interactuar en el ecosistema y acceder a sus servicios técnicos.

La adhesión es, por tanto, la puerta de entrada al ecosistema, y determina la relación inicial del participante con el espacio de datos, sus responsabilidades y las garantías bajo las cuales operará.

El flujo de adhesión debe garantizar:

- Identificación inequívoca de la organización solicitante.
- Validación de legitimidad y verificación documental por la autoridad del espacio de datos.
- Asignación de roles técnicas, capacidades y obligaciones.

- Emisión de credenciales verificables que representen las legitimaciones otorgadas.
- Registro oficial del participante en el Registro de Participantes.
- Generación de evidencias técnicas que permitan su auditoría posteros.

1. Actores y componentes implicados.

El flujo de adhesión implica los siguientes actores y servicios:

- Entidad solicitante, que desea integrarse como proveedor, consumidor u otro rol autorizado.
- Autoridad de gobernanza del espacio de datos, responsable de validar la solicitud y autorizar la incorporación.
- Servicio de identidad y credenciales verificables, encargado de emitir las legitimaciones técnicas.
- Registro de Participantes, encargado de almacenar la identidad, atributos y estado del participante.
- Módulo de observabilidad, que registra el proceso de adhesión para su auditoría posterior.

2. Secuencia operativa mínima.

La secuencia mínima del flujo de adhesión costa de las siguientes etapas:

- **Solicitud formal de adhesión**. La entidad se registra en el portal del ecosistema y proporciona documentación legal, técnica y organizativa que permita verificar su identidad y legitimidad.
- **Validación de identidad y legitimidad**. La autoridad de gobernanza verifica que la entidad cumple los criterios establecidos en el Libro de Reglas del espacio de datos.
- **Asignación de rol técnico y atributos asociados**. Se determina si el participante operará como proveedor, consumidor, intermediario, operador técnico u otro rol definido en el modelo de gobernanza. También se asigna atributos necesarios para su funcionamiento técnico.
- **Emisión de credenciales verificables**. El servicio de identidad genera credenciales verificables que representan los roles, atributos y legitimaciones otorgadas al participante. Estas credenciales serán utilizadas por los conectores y servicios habilitadores durante todos los flujos posteriores.
- **Inscripción en el Registro de Participantes**. La identidad, roles, atributos, estado y credenciales emitidas se almacenan en el Registro de forma íntegra, verificable y auditable.
- **Finalización de la adhesión y habilitación del participante**. La entidad pasa a estado “Activo” y queda habilitada para utilizar las capacidades técnicas del ecosistema.

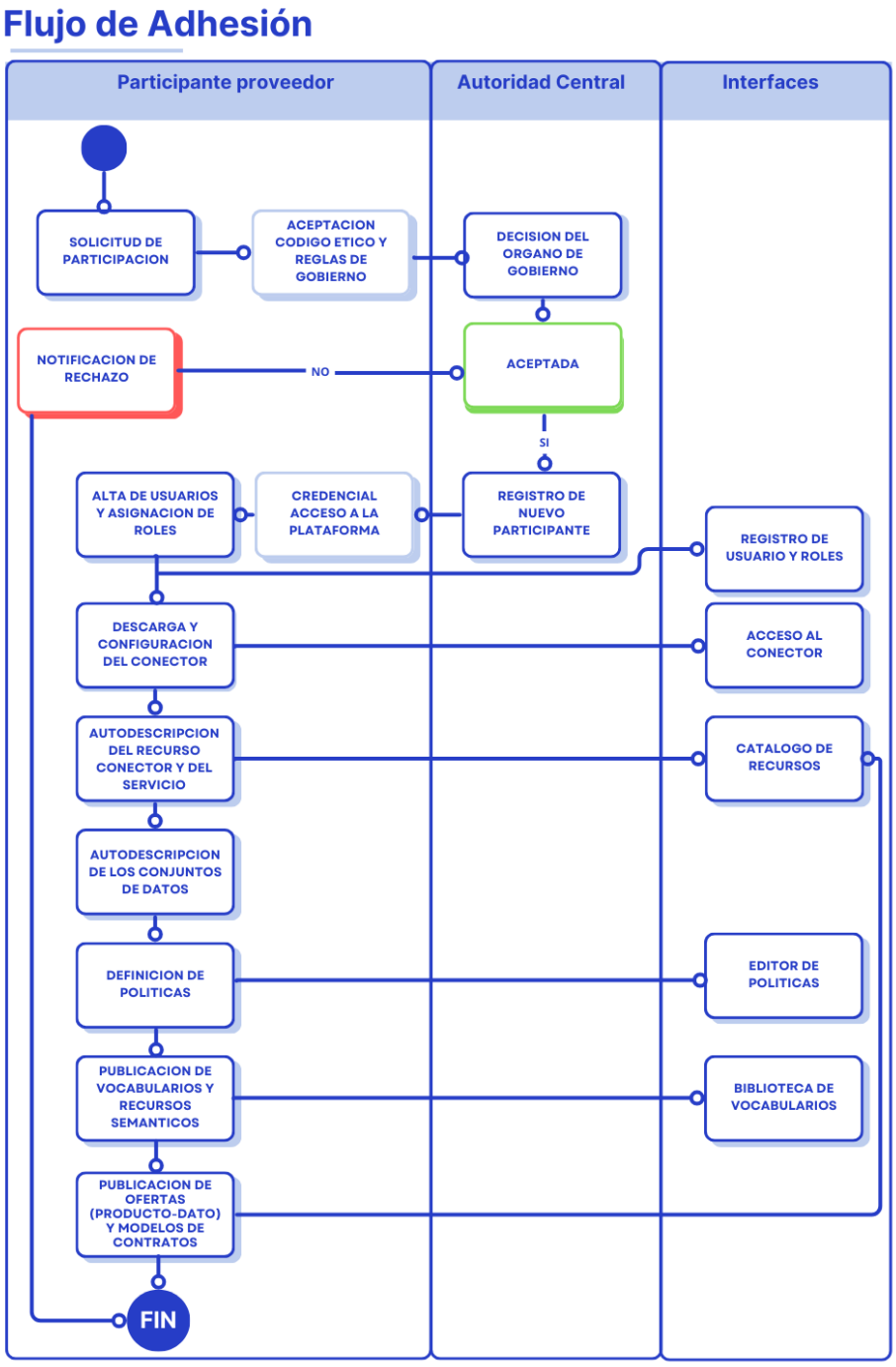


Ilustración 30: Flujo de adhesión

3. Reglas mínimas de interoperabilidad aplicables al flujo.

Para que el flujo sea considerado interoperable y conforme al marco, debe cumplir estas reglas:

- Toda identificación debe realizarse mediante mecanismos verificables.
- Toda validación debe generar evidencias estructuradas registradas en el módulo de observabilidad.
- La emisión de credenciales verificadas debe seguir un modelo de datos común y políticas estandarizadas.
- La inscripción el Registro debe garantizar integridad, disponibilidad y autenticación de los datos.
- Los roles y atributos asignados deben corresponderse con los definidos en la gobernanza técnica del ecosistema.

4. **Evidencias generadas durante el proceso.**

El flujo de adhesión debe dejar una traza completa y verificable, compuesta por la solicitud inicial, el resultado de la validación documental, los roles y atributos asignados, las credenciales verificables emitidas, la inscripción en el Registro y la resolución final de adhesión.

Estas evidencias serán empleadas en auditorías internas, verificaciones del Interoperability Hub y control de ciclo de vida del participante.

3.6.1.2. Publicación

La publicación de activos en el catálogo es uno de los flujos centrales del espacio de datos, ya que permite que los proveedores describan sus activos de manera estandarizada y que los consumidores puedan descubrirlos, evaluarlos y determinar si cumplen las necesidades.

La publicación debe garantizar coherencia, verificabilidad y trazabilidad. El proceso no cosiste únicamente en registrar un dataset, sino en aportar la información necesaria para que cualquier participante pueda descubrirlo, interpretarlo, evaluar su idoneidad, comprender sus restricciones y negociarlo.

La publicación debe garantizar:

- Metadatos completos y conformes a un modelo común, preferentemente DCAT-AP.
- Políticas de uso expresadas en formatos legibles por máquina, integradas mediante ODRL.
- Información sobre calidad, linaje y métodos de acceso, obligatoria para permitir evaluación previa.
- Trazabilidad del proceso de publicación, registrando evidencias que permitan auditorías futuras.
- Coherencia entre versión, estado del activo y políticas aplicables en cada momento.

1. **Actores y componentes implicados.**

- Proveedor de datos, responsable de crear, mantener y retirar los activos.
- Catálogo de recursos, que almacena sus descripciones, políticas, versiones y metadatos.

- Biblioteca de vocabulários, utilizada para validar modelos semânticos.
- Motor de políticas, encargado de validar la estructura y coherencia de las reglas ODRL.
- Módulo de observabilidad, que registra la operación.

2. Secuencia operativa mínima.

El flujo de publicación consta de las fases siguientes:

- **Preparación de la descripción del activo.** El proveedor elabora los metadatos del activo siguiendo un perfil DCAT-AP adaptado al ecosistema. La descripción debe incluir al menos los siguientes campos por recurso asociado: título, descripción, temas, responsable, formatos disponibles, modelo de acceso, calidad y linaje, políticas asociadas.
- **Validación estructural y semántica.** Antes de publicarse, la descripción debe superar controles automáticos: validación sintáctica mediante SHACL, verificación del cumplimiento del perfil adoptado (DCAT-AP), validación de coherencia semántica frente a los vocabularios disponibles y comprobación de la estructura de las políticas ODRL.
- **Registro y publicación en el catálogo.** Una vez validado, el activo se publica en el catálogo, asignándole: identificador único, fecha de publicación, versión, estado, políticas vigentes y enlace a distribuciones y servicios asociados.
- **Generación de evidencias.** El módulo de observabilidad registra: autor de la publicación, momento exacto, resultado de validaciones, políticas aplicadas, versión generada y evidencias criptográficas si procede.
- **Disponibilidad para descubrimiento.** Tras ser publicado, el activo queda disponible para consultas, filtros y búsquedas.

La siguiente ilustración muestra el flujo técnico de la publicación de activos en el espacio de datos:

Ilustración 31: flujo de publicación de activos en el Catálogo de recursos y Biblioteca de vocabularios.

3. Reglas mínimas de interoperabilidad aplicables al flujo.

Para considerar que un activo está publicado de forma interoperable, deben cumplirse los siguientes requisitos:

- Los metadatos deben seguir un modelo común y abierto.
- Las políticas de uso deben expresarse mediante un lenguaje estructurado, sin ambigüedades.
- Toda publicación debe generar evidencias técnicas.
- Toda política debe poder evaluarse automáticamente durante la negociación.
- La referencia al activo debe incluir su identidad y versionado.
- Los vocabularios utilizados deben proceder de la biblioteca de vocabularios del ecosistema.

4. Información mínima obligatoria

Se debe describir los activos y recursos asociados con información suficiente para permitir su evaluación técnica y semántica. La información mínima debe incluir: identidad del proveedor, políticas asociadas, situación jurídica del dato (si aplica), distribuciones

disponibles y condiciones de acceso, información técnica relevante (estructura, formatos, modos de uso), versión y fecha de actualización, nivel de calidad y métricas declaradas.

Categoría	Elemento	Obligatorio	Propósito
Identificación	Título, Identificador, Proveedor	Si	Identificación única
Descripción	Descripción, Temas, Etiquetas	Si	Evaluación de relevancia
Acceso	Endpoints, Formatos	Si	Descubrimiento operativo
Políticas	Permisos, Prohibiciones, Obligaciones (ODRL)	Si	Uso conforme
Calidad	DQV, métricas	Si	Evaluación de aptitud
Linaje	PROV-O	Recomendado	Trazabilidad
Versionado	Nº versión, Fecha	Si	Integridad y auditoría

Tabla 2. Metadatos mínimos obligatorios del recurso

5. **Gestión del ciclo de vida del activo.**

El proveedor sigue siendo soberano en la gestión del ciclo de vida del activo. Debe poder actualizarlo, modificar políticas, cambiar distribuciones, crear nuevas versiones y/o retirar un activo del catálogo.

La retirada del activo no debe eliminar evidencias previas, por razones de auditoría y trazabilidad.

3.6.1.3. Descubrimiento

El descubrimiento es el proceso mediante el cual los participantes localizan los activos publicados en el catálogo y determinan si cumplen con sus necesidades técnicas, semánticas, operativas o legales antes de iniciar una negociación. Este flujo es esencial para garantizar una interacción eficiente y transparente, y constituye la base sobre la que se establecen las condiciones de uso en la fase de negociación.

Los espacios de datos deben posibilitar mecanismos de descubrimiento homogéneos, basados en metadatos estandarizados y accesibles mediante interfaces abiertas. Este flujo no implica todavía acceso al dato, sino únicamente evaluación previa de su disponibilidad, sus características, sus políticas asociadas y sus posibles restricciones.

1. **Actores y componentes implicados.**

- Participante consumidor, que realiza la consulta.
- Catálogo de recursos, encargado de exponer los metadatos para la búsqueda.
- Biblioteca de vocabularios, utilizada para interpretar la semántica del recurso.
- Motor de políticas, que permite al consumidor visualizar o interpretar condiciones antes de negociar.
- Módulo de observabilidad, que restra las consultas realizadas, sin comprometer la privacidad de contenidos.

2. **Secuencia operativa mínima.**

El flujo consta de las siguientes fases:

- **Consulta al catálogo.** El participante consumidor inicia una búsqueda utilizando términos, filtros o criterios semánticos. El catálogo responde con los activos que cumplen los criterios, presentados mediante el perfil DCAT-AP.
- **Recuperación de la descripción completa del activo.** El consumidor accede a la ficha completa del activo y sus recursos asociados, que incluye: metadatos descriptivos, distribuciones disponibles, políticas ODRL asociadas, métricas de calidad (DQV), información de linaje (PROV-O), histórico de versiones, titularidad y responsabilidades.
- **Evaluación semántica.** El consumidor puede validar si los modelos de datos del recurso son compatibles con sus necesidades, consultando vocabularios utilizados, esquemas semánticos, **validaciones** SHACL y datos de referencia asociados.
- **Evaluación preliminar de políticas.** El consumidor revisa permisos, prohibiciones, obligaciones, restricciones de finalidad y limitaciones jurídicas o contractuales.
- **Evaluación técnica.** Se revisan aspectos relacionados con formatos disponibles, endpoints de acceso, modos de transferencia, frecuencia de actualización y requisitos de infraestructura.
- **Decisión de iniciar negociación.** Si el activo cumple con los criterios del participante este puede iniciar el flujo de negociación.

La siguiente imagen representa el flujo del descubrimiento:

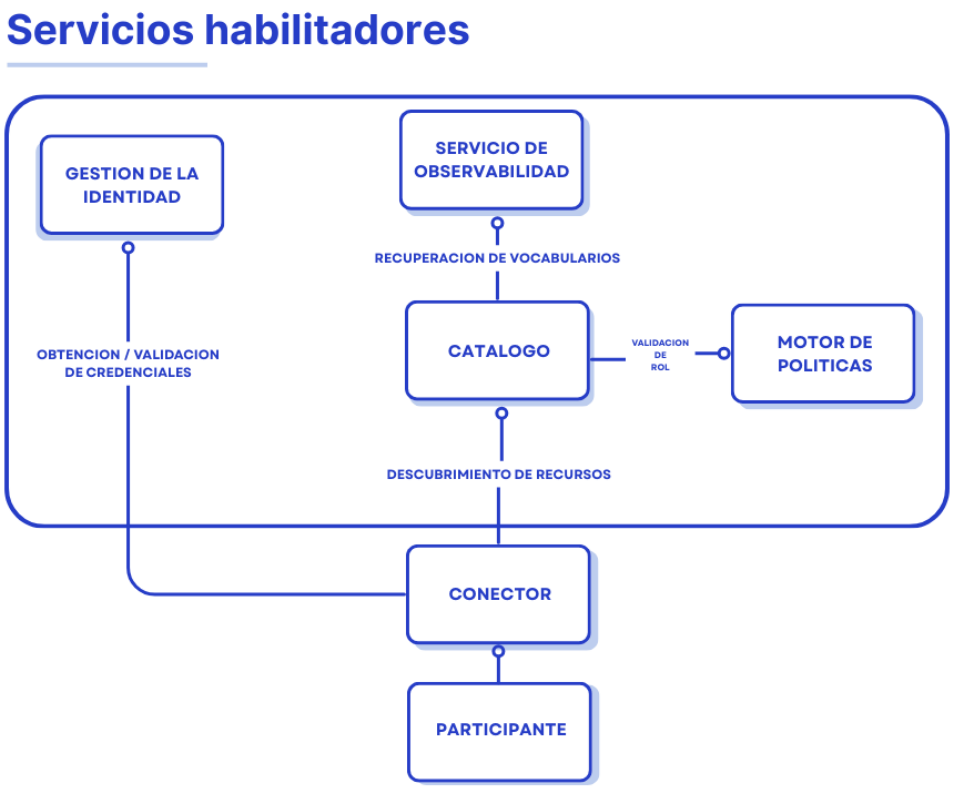


Ilustración 32: Cadena de

3. **Reglas mínimas de interoperabilidad aplicables al flujo.**

Para que el descubrimiento pueda considerarse interoperable, deben cumplirse las siguientes reglas:

- La consulta al catálogo debe realizarse mediante interfaces abiertas y documentadas.
- El catálogo debe devolver respuestas conformes con DCAT-AP y JSON-LD.
- Todas las políticas asociadas al activo deben estar disponibles de forma legible por máquina.
- El consumidor debe poder acceder a la descripción completa del activo sin restricciones, dado que esto no implica acceso al dato en sí.
- El proveedor debe garantizar que los metadatos están completos, actualizados y vinculados a una versión concreta del activo.
- Toda consulta debe generar evidencia técnica mínima en el módulo de observabilidad (sin registrar contenido sensible)

4. **Información mínima que debe poder recuperarse en el descubrimiento.**

La información mínima debe incluir:

- Descripción del activo. Título, propósito, dominio, temática, responsable.
- Información técnica. Formatos, esquemas, tipos de datos, modo de acceso.
- Políticas de uso. Permisos, prohibiciones, obligaciones, restricciones.
- Calidad. Métricas DQV, nivel de completitud, frecuencia de actualización.
- Linaje y procedencia. Modelado mediante PROV-O.
- Versionado y estado. Número de versión, fecha de publicación, vigencia de políticas.
- Identidad del proveedor. Datos de participante responsable del activo.

5. **Evidencias generadas durante el proceso.**

El descubrimiento debe registrar el identificador del participante consultante, la consulta realizada, el conjunto de activos recuperados, la ficha de activo consulta (ID), la fecha y hora y posibles incidencias semánticas o técnicas.

El registro de evidencias no debe almacenar datos personales o sensibles más allá de lo estrictamente necesario, en cumplimiento con la normativa aplicable y con los principios del ENS.

3.6.1.4. Negociación

La negociación es el proceso mediante el cual un participante consumidor solicita acceso a un activo publicado en el catálogo y acuerda con el proveedor las condiciones específicas bajo las cuales podrán utilizar dicho activo. Este flujo constituye el punto central de la gobernanza técnica, ya que vincula de manera formal las políticas declaradas por el proveedor con las obligaciones, restricciones y permisos que el consumidor acepta antes de que pueda producirse cualquier transferencia de datos.

La negociación debe basarse en información verificable, mecanismos de autenticación confiables, políticas expresadas en lenguajes legibles por máquina y decisiones técnicas reproducibles. Asimismo, la normativa europea en materia de acceso y uso de datos exige que los acuerdos de uso se documenten de forma clara, transparente y verificable, evitando interpretaciones ambiguas y garantizando el control efectivo de proveedor sobre la explotación del dato.

La negociación no implica todavía el acceso al dato, sino la formalización del marco contractual y técnico que habilitará la transferencia segura.

1. **Actores y componentes implicados.**

- Proveedor, titular del activo y soberano respecto a sus condiciones de uso.
- Consumidor, que solicita acceso al activo.
- Conectores de ambas partes, encargados de ejecutar el proceso técnico de negociación.
- Motor de políticas, que evalúa las reglas aplicables.
- Registro de Participantes, para validar roles y atributos.
- Módulo de identidad, para validar credenciales verificables.
- Módulo de observabilidad, que registra cada interacción durante el proceso.

2. **Secuencia operativa mínima.**

El flujo consta de las siguientes fases:

- **Solicitud de inicio de negociación.** El consumidor, tras evaluar un activo, envía a través de su conector una solicitud formal al proveedor, indicando: el recuso al que desea acceder, el propósito del acceso, la operación esperada (lectura, consulta, exportación, etc.) y los atributos relevantes del consumidor que puedan influir en la evaluación.
  Esta solicitud genera evidencia técnica inmediatamente.
- **Evaluación preliminar del proveedor.** El proveedor valida la identidad y rol de consumidor, revisa el propósito declarado, determina si la negociación es procedente según sus políticas, consulta el Registro para verificar atributos y obtiene información del motor de políticas.
  Si la solicitud es válida, el proveedor responde con una propuesta inicial de condiciones.
- **Intercambio de propuestas (negociación iterativa).** La negociación puede requerir varias iteraciones. Cada parte puede aceptar, rechazar o modificar políticas propuestas. La negociación puede incluir elementos como: permisos, prohibiciones, obligaciones, condiciones temporales o de caducidad, restricciones geográficas o de finalidad y compromisos de calidad o confidencialidad.
  Cada intercambio debe quedar registrado por el módulo de observabilidad.
- **Evaluación automática de políticas.** El motor de políticas evalúa la compatibilidad entre las políticas del proveedor, los atributos del consumidor, el propósito declarado y las restricciones del contrato.
  Las reglas deben evaluarse con un lenguaje estructurado como ODRL o XACML.
  Resultado posible:
  - Políticas compatibles → se puede establecer contrato.
  - Políticas incompatibles → negociación se rechaza.
- **Formalización del contrato de uso.** Una vez acordadas las condiciones, el proveedor y consumidor firman electrónicamente el contrato, se generan credenciales verificables de autorización, el contrato se registra con identificador único, estado y vigencia y se vinculan las políticas aplicables.
  Este contrato será utilizado por los conectores en el flujo de transferencia para autorizar o bloquear accesos.
- **Registro y cierre del proceso.** El módulo de observabilidad registra el acuerdo final, las versiones de las políticas aplicadas, las identidades y atributos utilizados, la evidencia de firma o aceptación y la vigencia temporal del contrato.

El consumidor queda autorizado a solicitar la transferencia de datos bajo los términos establecidos. La siguiente imagen muestra el flujo:

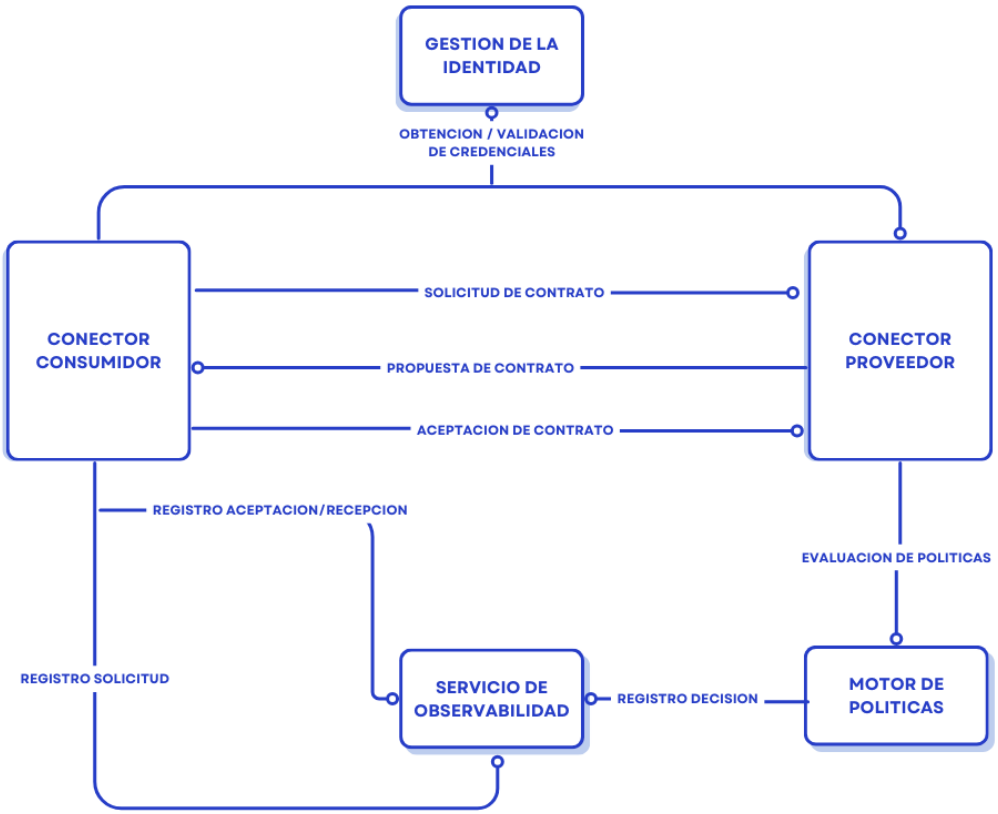


Ilustración 33: Secuencia de negociación

3. **Reglas mínimas de interoperabilidad aplicables al flujo.**

Para ser interoperable, este flujo debe cumplir:

- La identidad de ambos participantes debe estar verificada mediante credenciales válidas.
- Las políticas deben expresarse en formatos legibles por máquina y evaluables automáticamente.
- El contrato acordado debe generar evidencia registrable para auditoría.
- Ningún acceso al dato puede producirse sin un contrato válido y vigente.
- Toda negociación debe ser determinista: las mismas entradas dan los mismos resultados.
- Los conectores deben implementar la evaluación de políticas antes de solicitar la transferencia.

Estas reglas se traducirán posteriormente en requisitos MUST / SHOULD / MAY.

4. **Información mínima que debe gestionarse en la negociación.**

El proceso debe manejar, como mínimo:

- Identidad del proveedor y consumidor. Incluyendo sus atributos y roles asignados.

- Referencia inequívoca al activo. Dataset, distribución o servicio concretos.
- Políticas aplicables. Permisos, prohibiciones, obligaciones, condiciones temporales.
- Contrato resultante. Identificador, vigencia, condiciones aceptadas.
- Evidencias técnicas. Trazabilidad de mensaje, evaluaciones y decisiones.

Elemento	Descripción	Obligatorio
Identificador	ID único del contrato	Si
Participantes	Proveedor y consumidor	Si
Recurso(s)	Dataset / servicio negociado	Sí
Políticas	ODRL/XACML aplicables	Sí
Vigencia	Fecha de inicio y fin	Sí
Finalidad	Propósito declarado	Recomendado
Obligaciones	Condiciones exigidas	Si procede
Evidencias	Hash, sellos temporales	Si

Tabla 3. Información mínima del contrato de uso

5. **Evidencias generadas durante el proceso.**

La negociación debe generar evidencia verificable, incluyendo la solicitud inicial, propuestas y contraofertas, evaluaciones de políticas, validación de credenciales, contrato final firmado o aceptado y metadatos de la operación (hora, participantes, versiones).

Estas evidencias son imprescindibles para el control del cumplimiento, auditoría y certificación del Interoperability Hub.

3.6.1.5. Transferencia

La transferencia es el flujo mediante el cual el proveedor entrega un dato o servicio de datos a un consumidor bajo las condiciones establecidas en el contrato acordado. Constituye el punto de máxima criticidad operativa del ecosistema, ya que involucra la

circulación efectiva de datos, la aplicación estricta y la generación de evidencias técnicas verificables.

La UNE 0087:2025 establece que toda transferencia en un espacio de datos debe realizarse únicamente cuando:

- Existe un contrato válido y vigente.
- Se han verificado las identidades y loas atributos de ambos participantes.
- Se ha evaluado las políticas aplicables.
- El proveedor mantiene en todo momento el control sobre el ciclo de vida del dato.
- La interacción genera evidencias suficientes para permitir auditoría posterior.

Asimismo, el DGA y el Data Act exigen que los flujos de datos incluyan mecanismos de seguridad, trazabilidad, control de acceso y aplicación de restricciones, garantizando que solo pueden ejecutarse conforme a las condiciones pactadas entre las partes.

1. **Actores y componentes implicados.**

En la transferencia intervienen:

- Proveedor, que controla la operación.
- Consumidor, autorizado mediante contrato vigente.
- Conector del proveedor, que aplica políticas y controla la salida del dato.
- Conector del consumidor, que recibe el dato y aplica restricciones.
- Motor de políticas, que reevalúa condiciones antes y durante la transmisión.
- Servicio de identidad, que verifica credenciales y atributos.
- Módulo de observabilidad, que registra evidencia técnica del flujo.

2. **Secuencia operativa mínima.**

El flujo consta de las siguientes fases:

- **Inicio de la solicitud de transferencia.** El consumidor solicita el acceso al dato mediante su conector, referenciando el contrato vigente, el identificador del activo, el tipo de acceso solicitado (lectura, consulta, descarga, streaming, servicio) y el propósito previamente declarado.
- **Comprobaciones previas.** Antes de autorizar la salida del dato, el conector del proveedor debe realizar las siguientes verificaciones: validez del contrato (vigencia temporal, versión, ámbito de aplicación), identidad del consumidor y vigencia de credenciales verificables, compatibilidad de atributos (ABAC), políticas aplicables evaluadas mediante el motor de políticas, existencia de prohibiciones activas, restricciones de finalidad u obligaciones previas y coherencia entre políticas, contrato y solicitud técnica.
  Si cualquiera de estas verificaciones falla la transferencia se bloquea, se registra evidencia y se notifica la causa del consumidor.
- **Establecimiento del canal seguro.** Una vez superadas las verificaciones, los conectores establecen un canal seguro, cifrado y autenticado, que garantice confidencialidad (TLS 1.3), integridad del contenido, autenticación mutua y protección frente a ataques tipo replay o manipulación.

- **Aplicación de políticas en tiempo real.** Durante la transmisión, el conector del proveedor debe aplicar todas las restricciones del contrato incluyendo filtrados, limitaciones de tamaño o frecuencia, restricciones de campos, modificaciones obligatorias, anonimización/pseudonimización si aplica y reglas de acceso incremental o condicionado.
  El conector del consumidor debe respetar las obligaciones impuestas, tales como prohibición de redistribución, límites de reutilización, uso restringido a fines autorizados y controles de persistencia.
- **Transferencia efectiva del dato.** La transferencia puede adoptar distintos modelos: pull (cuando el consumidor solicita los datos), push (cuando el proveedor los envía proactivamente), streaming (cuando se trata de datos continuos) y Exchange de servicios (cuando el recurso es un API controlado).
  El proveedor mantiene siempre el control del proceso.
- **Registro de evidencias durante la transmisión.** El módulo de observabilidad debe registrar timestamp de cada fase, decisiones de políticas tomadas, tokens utilizados, metadatos del activo accedido, identificadores del contrato, tamaño y características de la transferencia y eventos de error, cancelación o error.
- **Finalización, cierre y obligaciones post-transmisión.** Una vez finalizada la transferencia el proveedor registra el resultado, el consumidor debe aplicar obligaciones, el sistema registra el estado final del flujo y se actualiza la trazabilidad del ciclo de vida del dato.

La siguiente ilustración muestra el flujo técnico de la transferencia:

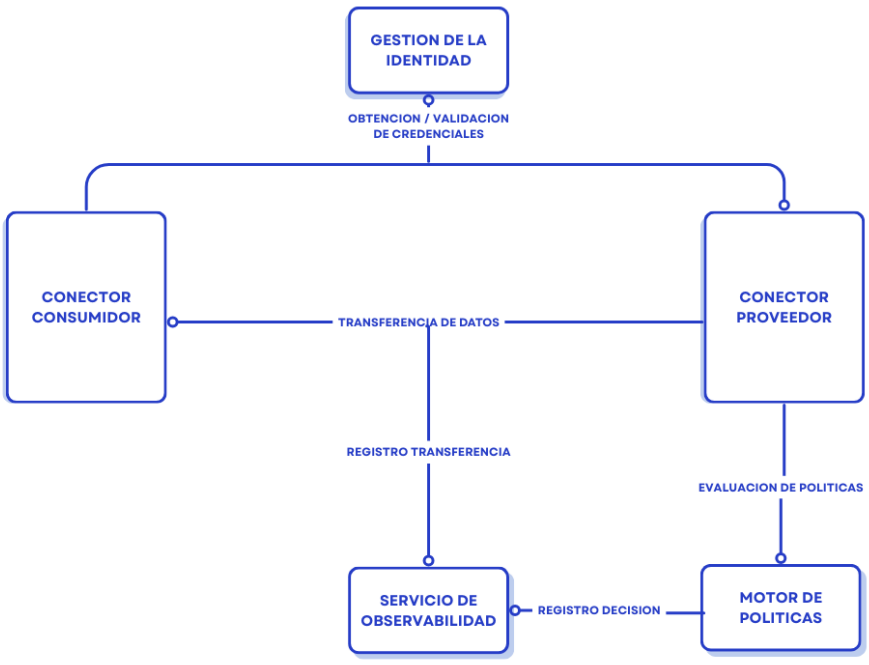


Ilustración 34: Secuencia de transferencia

3. **Reglas mínimas de interoperabilidad aplicables al flujo.**

Para considerar interoperable el flujo de transferencia, deben cumplirse los siguientes principios:

- Toda transferencia DEBE estar asociada a un contrato vigente.
- La identidad y atributos del consumidor DEBE verificar antes de transmitir datos.
- Las políticas de uso DEBE evaluarse antes y durante el flujo.
- Ningún dato PUEDE transferirse si existe incompatibilidad de políticas.
- La transferencia DEBERIA producir evidencias completas y verificables.
- Toda modificación, anonimización o filtrado DEBE registrarse.
- Los errores o interrupciones DEBE documentarse.
- El proveedor retiene siempre el control técnico del proceso.

4. **Garantías de soberanía técnica durante la transferencia**

El diseño del flujo debe asegurar que:

- El proveedor controla que se envía, cuándo, a quién y bajo qué condiciones.
- El consumidor sólo puede recibir y procesar datos conforme el contrato y las políticas vigentes.
- Las restricciones deben ser evaluables y verificables mediante políticas legibles por máquina.
- Toda acción debe poder ser reconstruida mediante evidencias técnicas.
- La arquitectura garantiza independencia tecnológica y cumplimiento del ENS.

5. **Evidencias generadas durante el proceso.**

El proceso de transferencia debe generar y conservar evidencias sobre identidad de participantes, contrato aplicado, políticas evaluadas, decisiones de autorización, eventos técnicos del flujo, integridad y cifrado y estado final de la operación.

3.6.1.6. Cierre, auditoría y ciclo de vida del dato

La fase de cierre constituye el último eslabón del flujo operativo de intercambio en un espacio de datos. Su función es asegurar que la transferencia realizada queda correctamente documentada, que se aplican las obligaciones posteriores al acceso, que las evidencias generadas permiten reconstruir el ciclo completo de la interacción y que la gobernanza técnica puede supervisar el cumplimiento de las condiciones acordadas en el contrato.

El cierre del flujo también constituye la fase que habilita la supervisión técnica continua, la recertificación de conectores y participantes y el funcionamiento del Interoperability Hub, que evaluará conformidad basándose en las evidencias registradas en cada etapa.

El cierre debe garantizar:

- La correcta finalización técnica de la transferencia.
- La aplicación de obligaciones posteriores al acceso.

- La generación y consolidación de evidencias verificables.
- La inscripción del resultado en los sistemas de observabilidad.
- La actualización del estado del contrato si corresponde.
- La integridad del ciclo de vida del dato, incluyendo su uso permitido y finalización.

Su propósito es asegurar que el proveedor mantiene soberanía sobre el ciclo de vida completo del dato, incluso después de haberlo transferido.

1. **Secuencia operativa mínima del cierre del flujo.**

El flujo consta de las siguientes fases:

- **Confirmación de finalización de la transferencia.** El proveedor confirma que la transferencia ha concluido correctamente, sin errores de integridad, autenticación o políticas. Esta confirmación queda registrada como evidencia.
- **Registro del estado final del flujo.** El módulo de observabilidad registra una entrada final que identifica el flujo, referencia el contrato utilizado, describe el estado final (éxito, error, cancelación, expiración) y vincula las evidencias generadas durante la transmisión.
- **Aplicación de obligaciones post-transferencia.** El consumidor debe cumplir las obligaciones derivadas del contrato, tales como restricciones de persistencia (borrado o caducidad), limitaciones de reutilización, restricciones de redistribución, obligaciones de anonimización o seudonimización y aplicación de medidas de seguridad equivalentes.
- **Actualización del ciclo de vida del dato.** El proveedor actualiza la información relativa al ciclo de vida: cuándo fue transferido, en qué condiciones, a quién y con qué restricciones.
  Esto es fundamental para reconstruir trazabilidad y justificar usos posteriores del activo.
- **Registro de auditoría y custodia de evidencias.** Todas las evidencias generadas en los pasos anteriores se consolidan en un repositorio de auditoría, garantizando su integridad mediante firmas electrónicas, hash de trazas, sellos de tiempo y técnicas de integridad del ENS.
- **Disponibilidad de evidencias para supervisión.** El Interoperability Hub o la autoridad de gobernanza deben poder consultar estas evidencias para verificar cumplimiento, diagnosticar incidencias técnicas, evaluar interoperabilidad o realizar auditorías periódicas.

2. **Reglas mínimas de interoperabilidad aplicables al cierre del flujo.**

El cierre debe cumplir, al menos, las siguientes reglas:

- La finalización de la transferencia DEBE generar evidencia estructurada.
- El módulo de observabilidad DEBE registrar un estado final del flujo.
- Todas las obligaciones post-transmisión DEBERÍA ser verificables mediante auditoría.
- La integridad de evidencias DEBE garantizarse mediante mecanismos criptográficos conformes al ENS.
- El contrato aplicable DEBERÍA actualizar su estado si lo requiere.

- El proveedor DEBE conservar prueba del cumplimiento o incumplimiento del consumidor.
- El consumidor DEBE ser capaz de demostrar cumplimiento de sus obligaciones cuando sea requerido.

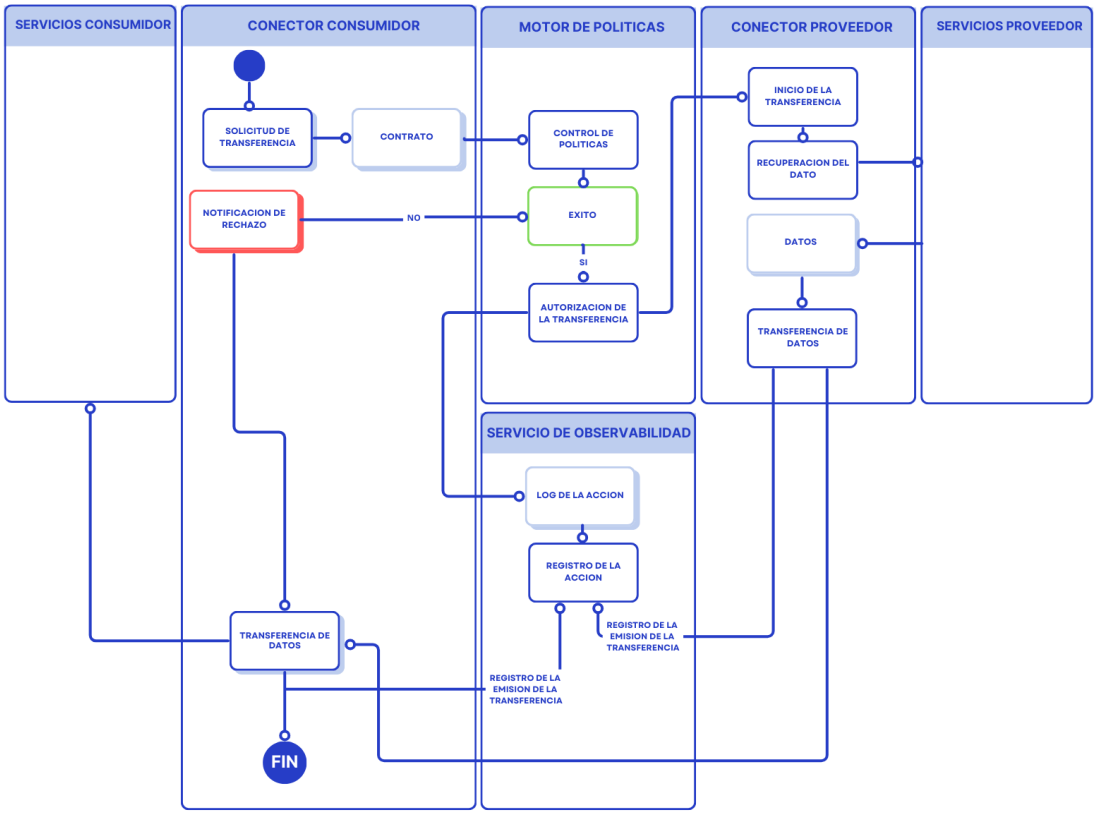


Ilustración 35: Secuencia de cierre y auditoría

3. Evidencias generadas durante el cierre.

Entre las evidencias mínimas se incluyen resultado de la transferencia, sellados temporales, roles aplicados y credenciales verificadas, políticas evaluadas, logs de decisiones técnicas, hash de trazas o paquetes, incidencias generadas durante la finalización y cumplimiento o incumplimiento de obligaciones post-transmisión.

4. Rol del Interoperability Hub en el cierre del flujo.

El Hub podrá utilizar esta fase para:

- Verificar la existencia y consistencia de las evidencias.
- Comprobar la aplicación correcta de políticas.
- Evaluar compatibilidad entre conectores.
- Certificar conformidad técnica del flujo.

- Detectar incumplimiento o anomalías.
- Generar informes de interoperabilidad.

Por ello, el diseño del flujo debe ser totalmente auditable y verificable, tanto para pruebas automatizadas como para auditorías externas.

3.6.2. Cómo interoperar entre varios espacios de datos

Como ya se ha definido al inicio de la sección *Interoperabilidad dentro y entre espacios de datos,* el intercambio de datos entre distintos dominios multiplica el valor potencial de los mismos, promoviendo la innovación, la optimización de la infraestructura y, en definitiva, impulsa el crecimiento económico.

Efectivamente, es de esperar que los participantes de un espacio de datos deseen acceder a los activos que se encuentran disponibles en otros espacios de datos, sectoriales o multidominio. Estos participantes se enfrentan, pues, al reto de construir las capacidades tecnológicas necesarias para cumplir con los distintos requisitos técnicos y normas de los espacios de datos en los que quieran participar.

La federación de los espacios de datos y la interoperabilidad entre ellos es clave para aumentar el valor generado a partir de los datos. No obstante, este paso se puede considerar una etapa de madurez mayor, que debe darse una vez los espacios de datos estén operativos y con un nivel de interoperabilidad interna demostrable y eficaz.

Habiendo llegado a un nivel de madurez óptimo por los diferentes espacios de datos, resulta de vital importancia reducir esta fuerte barrera de entrada. Para ello, las autoridades de gobierno deben abordar el diseño y creación de sus espacios de datos desde el paradigma de la interoperabilidad por diseño (*Interoperability-by-design*), priorizando la interoperabilidad con otros espacios de datos, siguiendo prácticas y marcos comunes, y ofreciendo servicios y funcionalidades consistentes con los que los participantes puedan sentirse cómodos y familiarizados.

Esto, a su vez, posibilitará una integración más fácil entre espacios de datos, posibilitando así la generación de sinergias entre múltiples dominios y, por ende, la generación de valor a partir de la puesta en marcha de casos de uso compartidos.

Para permitir a los participantes de sus respectivos espacios de datos intercambiar datos entre ellos sin necesidad de constituirse como participantes en cada uno de ellos, las autoridades de gobierno deben establecer un marco técnico, legal y de negocio común. Este marco común deberá:

1. **Asegurar el uso de un conjunto específico de estándares y protocolos** para implementar los principales procesos que soportan el intercambio de datos: el descubrimiento de datos, la negociación entre pares y la transferencia en sí de los datos.
2. **Establecer unos principios de gobernanza comunes**, que aseguren en todo momento la confianza y soberanía de los participantes, así como el cumplimiento de la normativa que les sea de aplicación.

3. **Estar basado en un entendimiento común de los casos de uso** a los que dan soporte, identificando aquellos componentes y servicios que puedan potenciar la generación de sinergias y la generación de valor.

Las subsecciones de este capítulo ahondan en estos aspectos, proporcionando una guía para establecer este marco común, detallando cómo las autoridades pueden definir las reglas que lo gobernarán, así como la base tecnológica que permitirá materializarlo.

3.6.2.1. Estándares y protocolos comunes

La interoperabilidad entre múltiples espacios de datos requiere algo más que la compatibilidad técnica a nivel de infraestructura o de formatos de datos. Para que los participantes de distintos espacios de datos puedan descubrir activos de manera federada, negociar contratos y compartir datos de manera segura y soberana, resulta imprescindible el uso de estándares y protocolos comunes que definan cómo interactúan entre sí.

En este contexto, los protocolos comunes actúan como una capa de interoperabilidad transversal, independiente de las implementaciones tecnológicas concretas de cada espacio de datos, y permiten la federación entre ecosistemas heterogéneos.

Cada espacio de datos puede estar construido con tecnologías, arquitecturas y proveedores distintos. Sin embargo, cuando dos espacios de datos desean interoperar, deben ser capaces de:

1. descubrir y entender los activos expuestos por el otro espacio,
2. negociar de forma automatizada las condiciones de acceso y uso de los datos,
3. aplicar y hacer cumplir políticas de uso acordadas,
4. garantizar la trazabilidad y la soberanía del dato durante todo el intercambio.

Es para cumplir con este fin que nacen protocolos como el **Dataspace Protocol** (DSP), promovido por IDSA y la Fundación Eclipse, que definen un lenguaje común de interacción entre conectores de espacios de datos, estandarizando los flujos básicos necesarios para la interoperabilidad:

- **Descubrimiento de activos y catálogos**: mecanismos para consultar y consumir catálogos de datos de otros espacios de datos de forma federada.
- **Negociación de contratos**: flujos estandarizados para la oferta, solicitud y formalización de acuerdos de intercambio de datos.
- **Referencia y aplicación de políticas de uso**: integración de políticas expresadas mediante lenguajes estándar (p. ej., ODRL) que regulan el acceso y el uso de los datos.
- **Control soberano del intercambio**: el proveedor mantiene el control sobre cuándo, cómo y bajo qué condiciones se accede a los datos, incluso tras la negociación del contrato.

Este protocolo no impone una implementación tecnológica concreta del conector, sino que garantiza que diferentes implementaciones puedan interoperar de forma consistente siempre que cumplan con la especificación.

En este contexto, se reconoce el middleware SIMPL como el referente tecnológico impulsado por la Comisión Europea para garantizar la interoperabilidad entre espacios de datos. En coherencia con esta visión europea, el Marco de Interoperabilidad Técnico continúa evolucionando hacia una nueva generación orientada a reforzar la interoperabilidad del ecosistema.

Protocolos semejantes permiten que:

- Diferentes espacios de datos sectoriales o regionales se federen entre sí.
- Conectores desarrollados por distintos proveedores o comunidades de código abierto puedan comunicarse.
- Se habilite un modelo de interoperabilidad N↔N, evitando integraciones punto a punto.

Esto resulta especialmente relevante en escenarios en los que coexistan múltiples espacios de datos impulsados por distintos actores, marcos regulatorios y dominios sectoriales.

El DSP se complementa con otros estándares y marcos comunes para asegurar que los espacios de datos no sean silos aislados, sino ecosistemas federados e interoperables. Varios de estos han sido mencionados anteriormente en este documento:

1. Modelos semánticos y de metadatos: DCAT-AP.
2. Expresión de políticas: ODRL.
3. Estándares para la gestión de identidad: Verifiable Credentials y eIDAS2.

Así mismo, resulta necesario un enfoque común para la gestión de la identidad de los participantes y de los servicios, que sea compatible con distintos modelos organizativos y de gobernanza. En particular, los espacios de datos deben poder operar en escenarios donde la identidad se gestione de forma centralizada, federada o descentralizada, sin comprometer la interoperabilidad ni la soberanía de los actores implicados.

Para ello, es fundamental adoptar estándares y protocolos abiertos que permitan verificar identidades, atributos y derechos de forma fiable, interoperable y reutilizable entre distintos espacios de datos.

Si se pretende construir un ecosistema en el que múltiples espacios de datos, la gestión de la identidad debe permitir:

- identificar de forma unívoca a organizaciones, servicios y componentes técnicos,
- verificar atributos relevantes (rol, afiliación, certificaciones, cumplimiento normativo),
- soportar distintos modelos de gobierno de identidad (centralizado, federado, descentralizado),
- reutilizar evidencias de identidad entre espacios de datos distintos,
- desacoplar la identidad de las implementaciones técnicas concretas.

Estos requisitos hacen inviable un enfoque basado exclusivamente en identidades locales o en integraciones punto a punto.

Es en este contexto en el que soluciones como los **Decentralised Identifiers (DID)** y las **Verifiable Credentials (VC)** cobran especial relevancia:

- Los DIDs proporcionan un mecanismo estandarizado para identificar de forma persistente y global a participantes y servicios, sin depender de una autoridad central única.
- Las VCs permiten expresar y verificar atributos (p.ej., identidad legal, pertenencia a un espacio de datos concreto, roles, etc.) asociados a una identidad de forma criptográficamente verificable.

Estas credenciales pueden posteriormente ser intercambiadas usando protocolos como:

- **OpenID for Verifiable Credentials (OID4VC):** define flujos estándar para la emisión, presentación y verificación de VC.
- **Data Space Credential Protocol (DCP)**: define flujos específicos para el uso de credenciales en interacciones propias de los espacios de datos, como la autenticación entre conectores y la verificación de atributos antes de la negociación.

En resumen, la combinación de DID, VC, OID4VC y DCP permite soportar de forma coherente distintos modelos de gestión de identidad:

- **Centralizado**: autoridades emisoras únicas y proveedores de identidad tradicionales.
- **Federado**: múltiples emisores reconocidos mutuamente entre espacios de datos.
- **Descentralizado**: control de la identidad por parte de los propios participantes, con verificación distribuida.

Este enfoque evita imponer un único modelo organizativo, facilitando la interoperabilidad entre espacios de datos con distintos grados de madurez y gobernanza.

3.6.2.2. Marco de gobernanza común

Los aspectos definidos anteriormente evidencian la necesidad de establecer estándares y principios de gobernanza comunes, asegurando un entendimiento compartido de las necesidades, usos y políticas. Establecer de forma efectiva la interacción entre espacios de datos y sus participantes requiere abordar específicamente aquellas dimensiones donde la falta de coordinación generaría fricción sistémica, duplicación de esfuerzos o erosión de la confianza entre espacios de datos.

No todos los aspectos de la gobernanza de un espacio de datos requieren el mismo nivel de coordinación. Mientras que muchos elementos pueden permanecer bajo la autonomía de cada espacio (estructuras organizativas, modelos de negocio específicos, políticas sectoriales particulares), existen tres dimensiones donde la coordinación no es opcional sino estructural para el funcionamiento del ecosistema: la federación de catálogos, el intercambio de datos y la gestión de la identidad.

Las tres dimensiones comparten una característica común: todas ellas implican puntos de contacto directo entre espacios de datos donde las diferencias no gobernadas se traducen

inmediatamente en incompatibilidades técnicas, ambigüedades legales o rupturas de confianza. Son las superficies de interacción donde la coherencia es indispensable.

Alcance y límite de la gobernanza

Gobernar la federación de catálogos, intercambio de datos y gestión de identidad no implica homogeneización total. Cada espacio de datos retiene amplios márgenes de autonomía para adaptar los mecanismos generales a sus particularidades.

- En la **federación de catálogos**, se establecen esquemas de metadatos nucleares y protocolos de consulta (p.ej. DCAT-AP), pero cada espacio puede extender los metadatos con campos específicos de su dominio, establecer sus propias políticas de visibilidad y decidir qué activos cataloga y cómo los organiza internamente.
- En el **intercambio de datos**, se definen formatos y protocolos preferentes y vocabularios para expresar condiciones de uso, pero cada espacio determina sus propias políticas sobre qué tipos de datos pueden compartirse, con qué nivel de procesamiento previo, bajo qué modelos de negocio y con qué requisitos de calidad documentados.
- En la **gestión de identidad**, se asegura que las identidades puedan federarse y que existan esquemas de atributos reconocibles (a través de soluciones técnicas como Decentralised Identifiers (DID) y las Verifiable Credentials (VC), pero cada espacio mantiene el control sobre sus propios proveedores de identidad, las políticas de registro de participantes, los roles específicos que define y los niveles de autorización que aplica internamente.

Operacionalización para la gobernanza entre espacios de datos

La gobernanza de las interacciones entre espacios de datos requiere del establecimiento de mecanismos que permitan, por parte de las autoridades de gobierno de cada uno de los ED implicados, el seguimiento y cumplimiento de las condiciones planteadas.

- **Marcos de reconocimiento mutuo**. Mecanismos mediante los cuales las autoridades de gobierno aceptan formalmente las decisiones, certificaciones o validaciones realizadas por otras autoridades en dominios específicos.
- **Mecanismos de escalado y resolución de conflictos**. Procedimientos que las autoridades de gobierno pueden invocar cuando surgen desacuerdos sobre interpretación de especificaciones, conflictos entre requisitos de diferentes espacios o problemas de interoperabilidad que no se resuelven a nivel técnico. Esto conlleva el planteamiento de mecanismos y procesos de mediación entre participantes de los diferentes espacios de datos, así como de arbitraje, de ser necesario.

Estos mecanismos se enmarcan en el contexto de las responsabilidades y funciones técnicas definidas en el Anexo B. Gobernanza técnica de la interoperabilidad. Entre ellos se encuentran aspectos clave como:

- **Cumplimiento normativo.** Conlleva asegurar el cumplimiento de las legislaciones comunes, así como de las específicas sectoriales cuando sea necesario. El objetivo es garantizar la interacción entre espacios sin generar inconsistencias legales.

- **Gestión de riesgos y seguridad:** deben contemplarse mecanismos que permitan identificar y mitigar los riesgos de seguridad derivados de la interacción entre participantes de los espacios de datos, principalmente aquellos relacionados con datos comprometidos.
- **Supervisión del ciclo de vida técnico:** que garantice el alineamiento y la coordinación respecto a actualizaciones técnicas, versionado de soluciones, evaluación de requisitos técnicos, así como la continuidad operativa.

El establecimiento de una gobernanza conjunta implica, además, la puesta en marcha de procesos e interfaces que permitan el alineamiento de cada uno de los espacios de datos con los acuerdos establecidos entre los espacios de datos mediante las respectivas autoridades de gobierno:

- Establecimiento de **puntos de contacto** por parte de las autoridades de gobierno asegurando:
  - Acuerdos y decisiones comunes puestos a disposición de los diferentes participantes.
  - Cobertura de las necesidades de los espacios de datos implicados y sus participantes.
  - Traducción de los acuerdos comunes a cambios dentro de los diferentes espacios de datos.
- Creación **procesos de alineamiento interno** que permitan y aseguren:
  - Análisis de impacto sobre los nuevos acuerdos o cambios requeridos en la colaboración. Principalmente en lo que respecta a la federación de catálogos, gestión de la identidad e intercambio de datos.
  - Actualización de procesos y documentos internos necesarios para garantizar la colaboración. Por ejemplo, el uso de estándares y especificaciones técnicas.
- Puesta en marcha de **mecanismos de retroalimentación** con los objetivos:
  - Gestión y reporte de incidencias relacionadas con la interacción entre los espacios de datos.
  - Fomentar la colaboración en el desarrollo de casos de uso exitosos que puedan ser replicables por otros espacios, ayudando en la generación de valor a través de los espacios de datos.

3.6.2.3. Federación de catálogos

Tal y como se ha mencionado en la sección relativa al Catálogo del espacio de datos, éste se constituye como uno de los principales pilares de este, siendo el punto de entrada para el descubrimiento del dato.

Para permitir el acceso a este a los participantes de los espacios de datos con los que la autoridad de gobernanza haya alcanzado acuerdos de colaboración, el Catálogo debe incluir capacidades que permitan compartir los datos que almacena con sus pares en los

otros espacios de datos. Estas capacidades se deben abordar teniendo en cuenta los siguientes aspectos:

1. El uso de un **protocolo común**.
2. El uso de **estándares comunes**, que establezcan la estructura de los metadatos descriptivos.
3. El uso de **credenciales verificables** por ambas partes.

Como se ha mencionado anteriormente, el Dataspace Protocol (DSP), establece un conjunto de especificaciones que permiten intercambiar datos entre partes en base a unas políticas específicas de control de acceso y uso. Estas especificaciones definen los esquemas y protocolos requeridos para la publicación y descubrimiento de los datos, así como para la negociación y acceso a los datos.

Para orquestar los intercambios entre participante y espacio de datos, y entre participantes, el DSP propone el uso de un Dataspace Connector (DSC), de manera similar a la planteada en este documento. Así mismo, el DSP establece el conector como el método de comunicación entre espacios de datos.

El diagrama a continuación ofrece una visión a alto nivel del proceso de descubrimiento y de los componentes involucrados en el mismo:

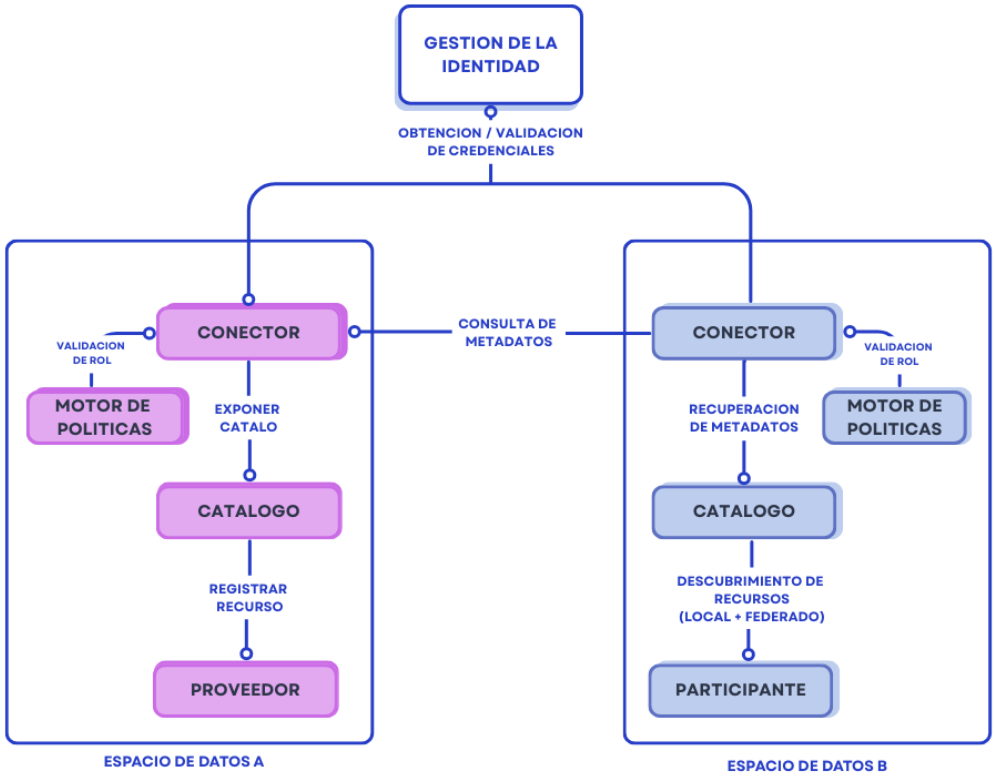


Ilustración 36: federación de catálogos entre espacios de datos.

1. El proveedor del espacio de datos A publica su activo en el Catálogo del espacio de datos A, tal y como se expone en el apartado 3.6.1.2.
2. El participante del espacio de datos B accede al catálogo de su espacio de datos, que confirma con el motor de políticas los atributos y rol del participante.
3. El conector del espacio de datos B se comunica con el conector del espacio de datos A para recuperar los metadatos de su catálogo.
4. El servicio de gestión de identidad garantiza la validez de las credenciales de ambos conectores.
5. El conector del espacio de datos A consiente el acceso al catálogo al conector del espacio de datos B a través de sus endpoints (ver Endpoints del Catálogo de Recursos), y tras validar sus atributos y rol.
6. El conector del espacio de datos B publica los metadatos en su catálogo.

3.6.2.4. Intercambio de datos

De manera similar a lo expuesto en el apartado anterior, para posibilitar la negociación y posterior intercambio de datos entre participantes de distintos espacios de datos, es indispensable que sus respectivos espacios cuenten con un protocolo, estándares y gestión de la identidad compatibles.

Como ya se ha detallado anteriormente, los conectores de los espacios de datos se erigen como la principal herramienta para posibilitar que el intercambio de datos se dé de manera segura, soberana y siempre cumpliendo con las políticas definidas de acceso y uso.

El diagrama a continuación describe este proceso entre participantes de distintos espacios de datos, y los componentes involucrados:

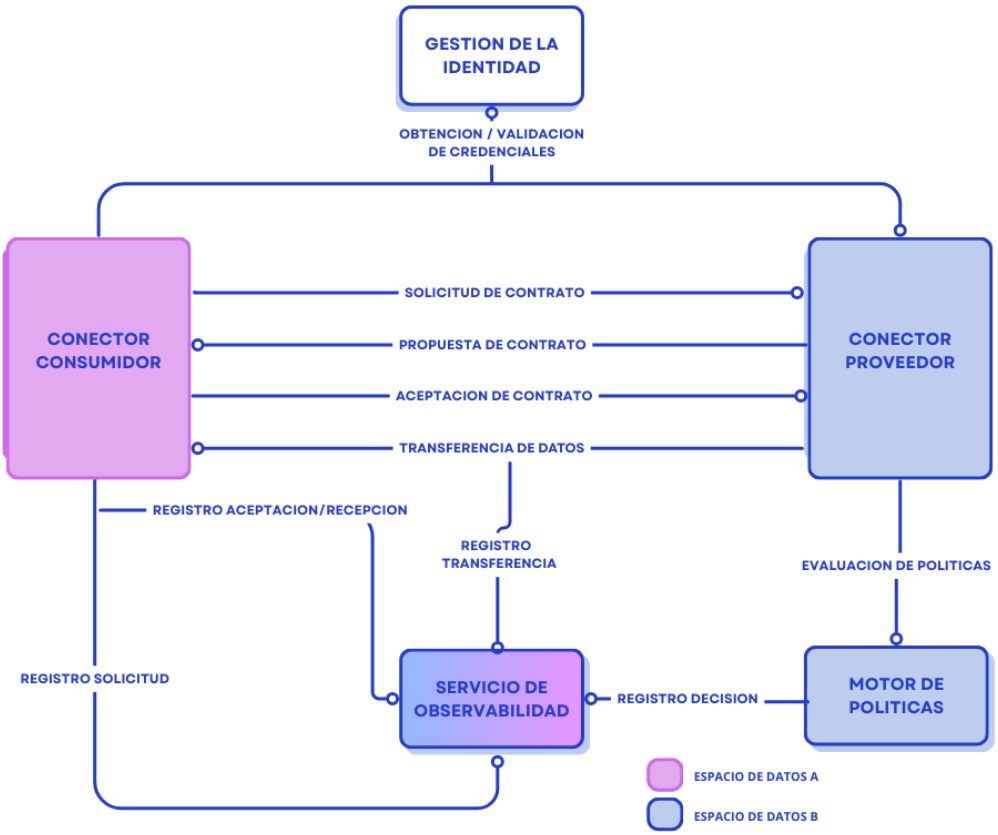


Ilustración 37: intercambio de datos entre participantes de distintos espacios de datos.

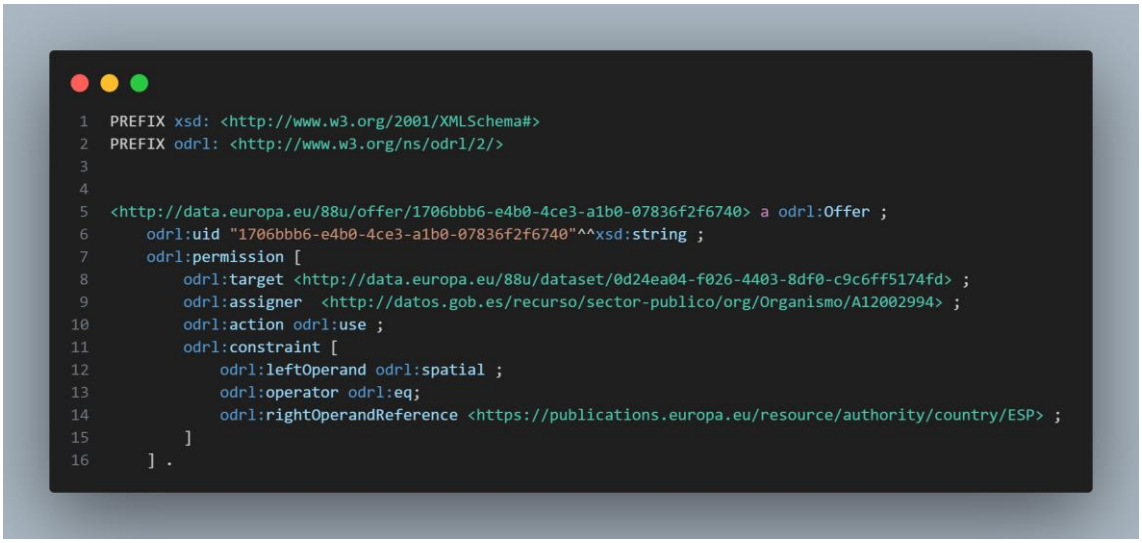
1. El conector consumidor del espacio de datos A solicita de formalización de un contrato sobre una oferta publicada por el conector proveedor del espacio de datos B.
2. El conector proveedor devuelve una propuesta de contrato al conector consumidor.
3. El conector consumidor devuelve la aceptación del contrato.
4. El contrato queda formalizado y todo el proceso registrado en los servicios de observabilidad de los dos espacios de datos.
5. Se inicia la transferencia, a petición de cualquiera de las partes o del proceso acordado (PULL, PUSH, *streaming*), que se autoriza por el Motor de políticas.

La sección Endpoints del Conector del Espacio de Datos detalla los endpoints usados en este proceso.

Para la descripción del contrato, ODRL cuenta con dos clases especializadas para representar el estado del contrato en sus diferentes estados:

1. **Offer**: usada para describir un conjunto de políticas no finales. Durante el proceso de negociación, se pueden intercambiar tantas instancias de esta clase como sean necesarias.
2. **Agreement**: usada para describir el conjunto de políticas finales que serán de aplicación sobre los recursos acordados y en las condiciones y periodo acordados.

El código a continuación representa un ejemplo de la clase Offer serializada en Turtle:



```
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX odrl: <http://www.w3.org/ns/odrl/2/>


<http://data.europa.eu/88u/offer/1706bbb6-e4b0-4ce3-a1b0-07836f2f6740> a odrl:Offer ;
    odrl:uid "1706bbb6-e4b0-4ce3-a1b0-07836f2f6740"^^xsd:string ;
    odrl:permission [
        odrl:target <http://data.europa.eu/88u/dataset/0d24ea04-f026-4403-8df0-c9c6ff5174fd> ;
        odrl:assigner  <http://datos.gob.es/recurso/sector-publico/org/Organismo/A12002994> ;
        odrl:action odrl:use ;
        odrl:constraint [
            odrl:leftOperand odrl:spatial ;
            odrl:operator odrl:eq;
            odrl:rightOperandReference <https://publications.europa.eu/resource/authority/country/ESP> ;
        ]
    ] .
```

Ilustración 38: ejemplo de clase Offer.

El ejemplo a continuación representa la clase Agreement. Las dos partes (odrl:Assigner y odrl:Asignee) han acordado que los datos solo pueden ser consumidos por una entidad establecida en España y únicamente hasta el 1 de enero de 2026:

```
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX odrl: <http://www.w3.org/ns/odrl/2/>

<http://data.europa.eu/88u/offer/1706bbb6-e4b0-4ce3-a1b0-07836f2f6740> a odrl:Agreement ;
    odrl:uid "1706bbb6-e4b0-4ce3-a1b0-07836f2f6740"^^xsd:string ;
    odrl:permission [
        odrl:target <http://data.europa.eu/88u/dataset/0d24ea04-f026-4403-8df0-c9c6ff5174fd> ;
        odrl:assigner <http://datos.gob.es/recurso/sector-publico/org/Organismo/A12002994> ;
        odrl:assignee <http://datos.gob.es/recurso/sector-publico/org/Organismo/E05229701> ;
        odrl:action odrl:use ;
        odrl:constraint [
            odrl:leftOperand odrl:spatial ;
            odrl:operator odrl:eq ;
            odrl:rightOperandReference <https://publications.europa.eu/resource/authority/country/ESP> ;
        ] ;
        odrl:constraint [
            odrl:leftOperand odrl:period ;
            odrl:operator odrl:le ;
            odrl:rightOperand "2026-01-01"^^xsd:dateTime
        ] ;
    ] .
```

Ilustración 39: ejemplo de odrl:Agreement.

4. Requisitos técnicos normativos (DEBE / DEBERÍA / PUEDE)

La interoperabilidad en un espacio de datos no puede garantizarse únicamente mediante la definición de una arquitectura común, la existencia de flujos operativos mínimos o la disponibilidad de servicios habilitadores. Para que el ecosistema funcione de forma homogénea, segura y verificable, es imprescindible disponer de un conjunto explícito de requisitos técnicos normativos que establezcan qué deben cumplir los participantes, los conectores y los distintos componentes del espacio de datos para considerarse conformes con el marco técnico.

La UNE 0087:2025 señala que los espacios de datos deben especificar requisitos mínimos que aseguren la correcta aplicación del modelo de gobernanza, permitan la interoperabilidad entre implementaciones heterogéneas y garanticen la trazabilidad del ciclo de vida del dato. Estos requisitos deben formularse de manera objetiva, comprensible y verificable, de modo que pueden utilizarse para evaluar el nivel de conformidad técnica de una solución, certificar un conector, validar un servicio habilitador o supervisar el comportamiento de un participante en cualquier fase del ciclo operativo.

Asimismo, el Esquema Nacional de Interoperabilidad (ENI) y el European Interoperability Framework (EIF) establecen que toda infraestructura interoperable debe basarse en criterios técnicos claros, definidos sobre estándares abiertos, que permitan evaluar la compatibilidad, la seguridad, la protección de la información y el cumplimiento de obligaciones. En el contexto del espacio de datos, estos criterios se traducen en condiciones normativas que afectan a la identidad digital, al registro de participantes, a la

catalogación de activos, a la negociación y transferencia de datos, a la aplicación automática de políticas y a la generación de evidencias técnicas.

El presente capítulo recoge estos requisitos utilizando la terminología normativa habitual en las especificaciones técnicas:

- DEBE (MUST), cuando se trate de una obligación imprescindible para asegurar la interoperabilidad o la soberanía del dato;
- DEBERÍA (SHOULD), cuando se recomiende una práctica técnica que aporta coherencia o robustez al ecosistema y cuya ausencia requiere justificación;
- PUEDE (MAY), cuando se permita flexibilidad en la implementación sin comprometer los principios esenciales del marco.

Estos requisitos permiten transformar el marco técnico en una especificación verificable, proporcionando la base para:

- Las evaluaciones de conformidad realizadas por la autoridad técnica,
- Los procesos de certificación de conectores y servicios habilitadores,
- Las pruebas de interoperabilidad en los entornos de sandbox,
- Las validaciones sistemáticas que ejecutará el futuro Interoperability Hub.

El capítulo se organiza en torno a cuatro bloques:

1. Requisitos por componente técnico, derivados directamente del Marco Técnico de Interoperabilidad.
2. Requisitos por proceso operativo, que garantizan que los flujos mínimos del espacio de datos pueden ejecutarse de forma uniforme y verificable.
3. Requisitos transversales, que aseguran seguridad, soberanía del dato, neutralidad tecnológica y portabilidad.
4. Acuerdos de interfaz y endpoints mínimos, que establecen las bases de integración que el Interoperability Hub utilizará para evaluar conformidad entre implementaciones.

Este capítulo debe entenderse como una guía de referencia rápida, diseñada para consulta frecuente y destinada a orientar tanto el diseño como la evaluación de las soluciones técnicas que operan en el espacio de datos.

4.1. Requisitos por componente técnico

4.1.1. Requisitos para la identidad y las credenciales verificables

La identidad verificable es la base de la confianza en el espacio de datos. Todos los participantes y componentes técnicos deben operar con credenciales emitidas y verificadas bajo un modelo común. Los siguientes requisitos garantizan autenticidad, atribución, trazabilidad y soberanía del dato en cualquier interacción.

Nº	Requisito	Nivel
ID-01	Toda organización y componente técnico que participe en el espacio de datos DEBE disponer de una identidad verificable basada en credenciales verificables.	DEBE
ID-02	Toda credencial verificable DEBE poder verificarse criptográficamente mediante un servicio común del espacio de datos.	DEBE
ID-03	La validación de identidad DEBE ejecutarse antes de cualquier operación crítica (publicación, descubrimiento, negociación o transferencia).	DEBE
ID-04	Los atributos utilizados para evaluar políticas (roles, legitimaciones, capacidades) DEBEN formar parte de credenciales verificables o estar registrados en el Registro de Participantes.	DEBE
ID-05	El servicio de identidad DEBE ofrecer mecanismos de revocación accesibles para todos los componentes del ecosistema.	DEBE
ID-06	Las credenciales verificables DEBERÍAN basarse en modelos y formatos abiertos (p. ej., W3C Verifiable Credentials).	DEBERÍA
ID-07	El ecosistema PUEDE aceptar identidades emitidas por otros espacios de datos bajo acuerdos de confianza compatibles.	PUEDE

Tabla 4. Requisitos para la identidad y las credenciales verificables

4.1.2. Requisitos para el Registro de Participantes

El Registro de Participantes es la fuente de verdad del espacio de datos respecto a quién participa, con qué rol, qué atributos posee y en qué estado operativo se encuentra. Sus requisitos normativos deben garantizar integridad, disponibilidad, coherencia con el servicio de identidad y trazabilidad completa del ciclo de vida de cada participante.

Nº	Requisito	Nivel
RP-01	El Registro DEBE mantener un listado único y actualizado de todos los participantes autorizados en el espacio de datos.	DEBE
RP-02	El Registro DEBE almacenar identidad verificable, roles técnicos y atributos relevantes para la evaluación de políticas.	DEBE

Nº	Requisito	Nivel
RP-03	La inscripción en el Registro DEBE realizarse únicamente tras la validación de identidad y legitimidad del participante.	DEBE
RP-04	El Registro DEBE exponer una API estándar que permita consultar el estado operativo de cualquier participante activo.	DEBE
RP-05	Toda modificación en roles, atributos o estado del participante DEBE registrarse con evidencia verificable en el sistema de observabilidad.	DEBE
RP-06	El Registro DEBERÍA sincronizar automáticamente los cambios de estado de credenciales emitidas por el servicio de identidad.	DEBERÍA
RP-07	El Registro PUEDE federarse con registros de otros espacios de datos, siempre que exista un modelo de confianza reconocido.	PUEDE

Tabla 5. Requisitos para el registro de participantes

4.1.3. Requisitos para el Catálogo de Recursos

El Catálogo de Recursos es el componente que permite publicar, describir y descubrir los activos del espacio de datos de forma estandarizada. Sobre él se apoyan los flujos de publicación, descubrimiento y negociación, por lo que sus requisitos deben asegurar descripciones completas, políticas legibles por máquina, validación semántica y trazabilidad de los cambios.

Nº	Requisito	Nivel
CR-01	El Catálogo DEBE implementar un perfil DCAT-AP adaptado al espacio de datos para describir todos los activos y recursos publicados.	DEBE
CR-02	Todo recurso publicado DEBE incluir metadatos mínimos obligatorios: identificación del proveedor, descripción, acceso, políticas, calidad y versión.	DEBE
CR-03	Las políticas de uso asociadas a un activo DEBEN expresarse mediante un lenguaje legible por máquina (p. ej., ODRL).	DEBE
CR-04	Los metadatos del activo y recursos asociados DEBEN someterse a validación estructural y semántica antes de su publicación (p. ej., SHACL + vocabularios del ED).	DEBE

Nº	Requisito	Nivel
CR-05	El Catálogo DEBE exponer interfaces abiertas para búsqueda, filtrado y consulta de activos (API de descubrimiento).	DEBE
CR-06	Toda publicación, actualización o retirada de un activo DEBE generar evidencia técnica registrada en el sistema de observabilidad.	DEBE
CR-07	Las descripciones del Catálogo DEBERÍAN utilizar formatos interoperables (RDF/JSON-LD) y vocabularios comunes del ecosistema.	DEBERÍA

Tabla 6. Requisitos para el catálogo de recursos

4.1.4. Requisitos para la Biblioteca de Vocabularios

La Biblioteca de Vocabularios es el repositorio semántico oficial del espacio de datos. Garantiza que los recursos se describen con un significado homogéneo y verificable, permitiendo que los participantes interpreten los datos de forma consistente. Esta sección recoge los requisitos mínimos que debe cumplir para asegurar la interoperabilidad semántica.

Nº	Requisito	Nivel
BV-01	La Biblioteca de Vocabularios DEBE almacenar y publicar los vocabularios, taxonomías y modelos semánticos utilizados en el espacio de datos.	DEBE
BV-02	La validación semántica de metadatos del Catálogo DEBE realizarse utilizando vocabularios registrados en esta Biblioteca.	DEBE
BV-03	La Biblioteca DEBE ofrecer APIs para consulta, descarga y versionado de vocabularios y esquemas.	DEBE
BV-04	Los vocabularios DEBEN mantenerse versionados, con trazabilidad completa de actualizaciones y retiradas.	DEBE
BV-05	La Biblioteca DEBERÍA permitir enlazar vocabularios externos (nacionales, europeos o sectoriales) mediante federación o alineación.	DEBERÍA
BV-06	La Biblioteca DEBERÍA ofrecer mecanismos para verificar la coherencia semántica de recursos (p. ej., validación SHACL).	DEBERÍA

Nº	Requisito	Nivel
BV-07	La Biblioteca PUEDE soportar múltiples formatos de representación (RDF, JSON-LD, TTL), según las necesidades del ecosistema.	PUEDE

Tabla 7. Requisitos para la biblioteca de vocabularios

4.1.5. Requisitos para el Conector del espacio de datos

El conector es el componente técnico mediante el cual los participantes ejecutan los procesos de negociación, autorización y transferencia de datos. Actúa como pasarela segura entre organizaciones, aplicando las políticas del espacio de datos y garantizando trazabilidad.

Los siguientes requisitos recogen el mínimo imprescindible para asegurar interoperabilidad efectiva entre participantes y entre espacios de datos.

Nº	Requisito	Nivel
CO-01	El conector DEBE autenticar y autorizar todas las solicitudes utilizando identidades y credenciales verificables emitidas por el espacio de datos.	DEBE
CO-02	El conector DEBE consultar el Registro de Participantes para verificar el estado, rol y atributos de la contraparte antes de iniciar cualquier interacción.	DEBE
CO-03	El conector DEBE invocar al Motor de Políticas para evaluar permisos, prohibiciones y obligaciones antes de iniciar la negociación y la transferencia.	DEBE
CO-04	El conector DEBE establecer canales seguros (TLS 1.3 o equivalente) para toda transferencia, garantizando confidencialidad, integridad y autenticación mutua.	DEBE
CO-05	El conector DEBE aplicar de forma automática las restricciones del contrato (filtros, anonimización, límites de uso, finalidades, etc.) durante la transferencia.	DEBE
CO-06	Todas las acciones críticas del conector (autenticación, negociación, transferencia, errores) DEBEN generar evidencias verificables en el módulo de observabilidad.	DEBE

Nº	Requisito	Nivel
CO-07	El conector DEBERÍA soportar múltiples modos de transferencia (pull, push, streaming, servicio) según las capacidades declaradas por el proveedor.	DEBERÍA
CO-08	El conector PUEDE implementar mecanismos adicionales de optimización o control siempre que no vulneren políticas ni alteren la trazabilidad exigida.	PUEDE

Tabla 8. Requisitos para el conector del espacio de datos

4.1.6. Requisitos para Políticas y Contratos legibles por máquina

Las políticas y contratos legibles por máquina permiten que el espacio de datos aplique de forma automática las reglas del Marco de Gobernanza y las condiciones acordadas entre proveedor y consumidor. Constituyen la base para la negociación, la autorización y la transferencia controlada del dato.

Los siguientes requisitos establecen el mínimo esencial para garantizar interoperabilidad jurídica y técnica en un entorno automatizado.

Nº	Requisito	Nivel
PC-01	Las políticas de uso de un recurso DEBEN expresarse mediante un lenguaje legible por máquina (p. ej., ODRL o equivalente).	DEBE
PC-02	Las políticas DEBEN definir permisos, prohibiciones y obligaciones de forma explícita y no ambigua.	DEBE
PC-03	Las políticas y atributos utilizados en la negociación DEBEN basarse en vocabularios estandarizados y registrados en la Biblioteca de Vocabularios del ED.	DEBE
PC-04	La evaluación de políticas DEBE ser determinista: mismas entradas → mismo resultado.	DEBE
PC-05	El contrato técnico resultante de la negociación DEBE incluir: participantes, recurso, políticas acordadas, vigencia y evidencias mínimas.	DEBE

Nº	Requisito	Nivel
PC-06	Las políticas DEBERÍAN permitir la inclusión de condiciones dinámicas (finalidad, contexto, territorio, volumen, ventanas temporales).	DEBERÍA
PC-07	El espacio de datos PUEDE admitir múltiples lenguajes de políticas si su interpretación puede resolverse en un modelo común evaluable.	PUEDE

Tabla 9. Requisitos para políticas y contratos legibles por máquina

4.1.7. Requisitos para Observabilidad, auditoría y evidencias

La observabilidad y la auditoría técnica permiten reconstruir lo que ocurre en el espacio de datos, verificar cumplimiento de políticas, resolver disputas, detectar anomalías y proporcionar información. Este componente es esencial para asegurar transparencia, responsabilidad y soberanía técnica en todos los flujos del ecosistema.

Nº	Requisito	Nivel
OB-01	El espacio de datos DEBE registrar evidencias verificables de todas las interacciones críticas (adhesión, publicación, negociación, transferencia y cierre).	DEBE
OB-02	El módulo de observabilidad DEBE exponer una API para el registro estructurado de eventos (identidad, timestamp, política evaluada, decisión, resultado).	DEBE
OB-03	Toda evidencia generada DEBE garantizar integridad, autenticidad y sellado temporal conforme al ENS.	DEBE
OB-04	El sistema de auditoría DEBE permitir reconstruir el flujo completo de una operación mediante correlación de eventos.	DEBE
OB-05	Las trazas registradas DEBERÍAN utilizar formatos interoperables (JSON-LD, RDF) que permitan análisis automatizado.	DEBERÍA
OB-06	El módulo de observabilidad DEBERÍA permitir consultas autenticadas para análisis, supervisión y comprobaciones de cumplimiento.	DEBERÍA

Nº	Requisito	Nivel
OB-07	El sistema PUEDE ofrecer capacidades avanzadas de monitorización (alertas, agregaciones, detección de anomalías) para mejorar la supervisión del ecosistema.	PUEDE

Tabla 10. Requisitos para observabilidad, auditoría y evidencias

4.2. Requisitos por los procesos mínimos

Los flujos operativos mínimos garantizan que cualquier espacio de datos funcione de manera homogénea, verificable y conforme a las reglas del Marco de Gobernanza.

Los siguientes requisitos representan el nivel mínimo de interoperabilidad exigible a los implementadores del ecosistema.

4.2.1. Requisitos para el Flujo de Adhesión

El flujo de adhesión garantiza que solo organizaciones legítimas y verificadas puedan operar en el espacio de datos. A través de este proceso se valida la identidad del solicitante, se asignan roles técnicos y se emiten credenciales verificables que permitirán su interacción con el ecosistema bajo un marco de confianza y trazabilidad.

Nº	Requisito	Nivel
FL-A-01	La identidad de la entidad solicitante DEBE verificarse mediante credenciales verificables válidas.	DEBE
FL-A-02	La autoridad del ED DEBE validar legitimidad y documentación antes de autorizar la adhesión.	DEBE
FL-A-03	La asignación de roles y atributos técnicos DEBE registrarse en el Registro de Participantes.	DEBE
FL-A-04	La emisión de credenciales verificables DEBE seguir un modelo de datos común.	DEBE
FL-A-05	Todo el proceso de adhesión DEBE generar evidencias verificables en el módulo de observabilidad.	DEBE
FL-A-06	La adhesión DEBERÍA permitir presentación selectiva de atributos cuando sea posible.	DEBERÍA

Tabla 11. Requisitos para el Flujo de Adhesión

4.2.2. Requisitos para el Flujo de Publicación

La publicación permite que los proveedores describan sus activos mediante un modelo de metadatos común, asegurando coherencia, verificabilidad y descubrimiento homogéneo. Este flujo establece las bases semánticas y políticas que condicionarán la evaluación, negociación y transferencia de los activos.

Nº	Requisito	Nivel
FL-P-01	Los metadatos de un activo y recursos asociados DEBEN cumplir un perfil DCAT-AP adaptado al ED.	DEBE
FL-P-02	Las políticas del activo DEBEN expresarse en un lenguaje legible por máquina (ODRL).	DEBE
FL-P-03	La publicación DEBE validar estructura y semántica (SHACL + vocabularios del ED).	DEBE
FL-P-04	Toda publicación, actualización o retirada DEBE generar evidencias registradas.	DEBE
FL-P-05	El catálogo DEBE exponer el activo inmediatamente tras su validación.	DEBE
FL-P-06	El proveedor DEBERÍA incluir métricas de calidad y linaje (PROV-O).	DEBERÍA

Tabla 12. Requisitos para el flujo de publicación

4.2.3. Requisitos para el Flujo de Descubrimiento

El flujo de descubrimiento habilita que los consumidores localicen y analicen los activos disponibles en el espacio de datos. Permite evaluar sus características técnicas, semánticas y políticas de uso antes de iniciar cualquier interacción contractual o transferencia de datos.

Nº	Requisito	Nivel
FL-D-01	Las consultas al catálogo DEBEN realizarse mediante interfaces abiertas.	DEBE

Nº	Requisito	Nivel
FL-D-02	El catálogo DEBE devolver resultados en formatos interoperables (DCAT-AP/JSON-LD).	DEBE
FL-D-03	Las políticas asociadas al activo DEBEN estar disponibles para evaluación previa.	DEBE
FL-D-04	La ficha completa del activo DEBE ser accesible sin restricciones (sin acceso al dato).	DEBE
FL-D-05	El flujo de descubrimiento DEBE generar evidencia mínima en observabilidad.	DEBE
FL-D-06	El descubrimiento DEBERÍA permitir filtrado semántico mediante vocabularios del ED.	DEBERÍA

Tabla 13. Requisitos para el flujo de descubrimiento

4.2.4. Requisitos para el Flujo de Negociación

La negociación establece las condiciones técnicas y contractuales bajo las cuales un consumidor podrá acceder y utilizar un activo. Este flujo materializa la aplicación automática de políticas, la verificación de atributos y la formalización del contrato técnico que habilitará la transferencia.

Nº	Requisito	Nivel
FL-N-01	El conector DEBE autenticar a ambas partes mediante credenciales verificables.	DEBE
FL-N-02	Las políticas declaradas por el proveedor DEBEN evaluarse automáticamente antes del acuerdo.	DEBE
FL-N-03	El resultado de la negociación DEBE formalizarse en un contrato técnico legible por máquina.	DEBE
FL-N-04	El contrato DEBE incluir participantes, activo, políticas, atributos y vigencia.	DEBE
FL-N-05	Todos los intercambios de propuestas DEBEN registrarse como evidencias.	DEBE

Nº	Requisito	Nivel
FL-N-06	La negociación DEBERÍA ser determinista (mismas entradas → mismo resultado).	DEBERÍA

Tabla 14. Requisitos para el flujo de negociación

4.2.5. Requisitos para el Flujo de Transferencia

El flujo de transferencia ejecuta el intercambio de datos bajo las condiciones previamente negociadas, garantizando seguridad, soberanía del dato, evaluación técnica de restricciones y generación de evidencias verificables durante toda la operación

Nº	Requisito	Nivel
FL-T-01	La transferencia DEBE asociarse a un contrato válido y vigente.	DEBE
FL-T-02	El conector del proveedor DEBE validar identidad, atributos y políticas antes de transferir.	DEBE
FL-T-03	La transferencia DEBE realizarse mediante un canal seguro (TLS 1.3 o equivalente).	DEBE
FL-T-04	El conector DEBE aplicar automáticamente restricciones contractuales durante la transmisión.	DEBE
FL-T-05	Todos los eventos del flujo DEBEN registrarse con evidencias verificables.	DEBE
FL-T-06	La transferencia DEBERÍA soportar diferentes modos (*pull*, *push*, *streaming*) según el activo.	DEBERÍA
FL-T-01	La transferencia DEBE asociarse a un contrato válido y vigente.	DEBE

Tabla 15. Requisitos para el flujo de transferencia

4.2.6. Requisitos para el Cierre / ciclo de vida

El cierre consolida las evidencias generadas durante la transferencia, verifica el cumplimiento de obligaciones posteriores al acceso y actualiza el estado contractual y de

ciclo de vida del dato. Este flujo habilita supervisión, auditoría y certificación del comportamiento técnico del ecosistema.

Nº	Requisito	Nivel
FL-C-01	La finalización de la transferencia DEBE generar un evento de cierre con estado final.	DEBE
FL-C-02	El consumidor DEBE aplicar las obligaciones post-uso definidas en el contrato (borrado, no redistribución, restricciones de finalidad).	DEBE
FL-C-03	Todas las evidencias del flujo DEBEN consolidarse en el sistema de auditoría con integridad garantizada.	DEBE
FL-C-04	El proveedor DEBE mantener trazabilidad completa del ciclo de vida del activo intercambiado.	DEBE
FL-C-05	Los registros de auditoría PUEDEN incluir sellados temporales avanzados o pruebas adicionales de integridad.	PUEDE

Tabla 16. Requisitos para el cierre / ciclo de vida

4.3. Requisitos transversales

4.3.1. Requisitos para la Seguridad y soberanía del dato

La seguridad y la soberanía del dato son principios estructurales del espacio de datos. Garantizan que cada participante mantiene control sobre sus activos y que cualquier intercambio se realiza de forma segura, conforme a políticas, bajo contrato y con trazabilidad completa. Los siguientes requisitos recogen el núcleo mínimo que debe implementarse para cumplir UNE 0087:2025, ENS y la normativa europea (DGA, Data Act)

Nº	Requisito	Nivel
SS-01	Todo intercambio de datos DEBE estar respaldado por un contrato técnico válido y verificable.	DEBE
SS-02	La transferencia de datos DEBE realizarse mediante canales seguros que garanticen cifrado, autenticación mutua e integridad.	DEBE
SS-03	El proveedor DEBE mantener control técnico sobre qué datos se transfieren, a quién, bajo qué condiciones y durante cuánto tiempo.	DEBE

Nº	Requisito	Nivel
SS-04	Las obligaciones post-uso (retención, borrado, no redistribución, limitación de finalidad) DEBEN poder aplicarse y auditarse.	DEBE
SS-05	Las políticas aplicables a un activo DEBEN evaluarse automáticamente antes y durante la transferencia.	DEBE
SS-06	Los mecanismos de custodia y sellado temporal de evidencias DEBERÍAN cumplir requisitos del ENS.	DEBERÍA
SS-07	El espacio de datos PUEDE adoptar mecanismos adicionales de soberanía (p. ej., restricciones geográficas o de infraestructura).	PUEDE

Tabla 17. Requisitos para la seguridad y soberanía del dato

4.3.2. Requisitos para la Compatibilidad, portabilidad y neutralidad tecnológica

El espacio de datos debe poder integrarse en múltiples entornos tecnológicos, evolucionar sin generar dependencias y facilitar la interoperabilidad entre soluciones heterogéneas. Estos requisitos establecen las bases de compatibilidad y neutralidad necesarias para garantizar libertad tecnológica, portabilidad de componentes y continuidad operativa en el ecosistema.

Nº	Requisito	Nivel
CP-01	Los componentes del espacio de datos DEBEN basarse en estándares abiertos y ampliamente adoptados.	DEBE
CP-02	La arquitectura del ED DEBE permitir que sus componentes se desplieguen en entornos on-premise, cloud o híbridos sin pérdida de funcionalidad.	DEBE
CP-03	Los componentes DEBEN exponer interfaces abiertas (APIs) definidas en el Marco Técnico y documentadas públicamente.	DEBE
CP-04	La arquitectura DEBERÍA permitir sustituir un componente por otro equivalente sin afectar al resto del ecosistema.	DEBERÍA
CP-05	Los participantes DEBERÍAN poder migrar sus conectores y servicios habilitadores entre entornos sin reconfiguraciones complejas.	DEBERÍA

Nº	Requisito	Nivel
CP-06	El ecosistema PUEDE admitir componentes alternativos o ampliados, siempre que respeten interfaces y políticas del ED.	PUEDE
CP-07	Los mecanismos de versionado DEBEN garantizar compatibilidad progresiva entre versiones de APIs y modelos de datos.	DEBE

Tabla 18. Requisitos para la compatibilidad, portabilidad y neutralidad tecnológica

4.4. Capacidades de interfaz y endpoints de referencia

Los siguientes acuerdos de interfaz describen un conjunto de **capacidades técnicas de referencia** que pueden facilitar la interoperabilidad entre implementaciones dentro de un espacio de datos.

Estos elementos se presentan como una **guía orientativa de capacidades mínimas**, y no deben interpretarse como una especificación normativa cerrada ni como una obligación estricta de implementación. Su objetivo es proporcionar un **punto común de referencia técnica** que permita alinear desarrollos, facilitar la compatibilidad entre soluciones y servir como punto de partida para la evaluación de interoperabilidad.

Las implementaciones pueden adoptar enfoques alternativos, siempre que garanticen capacidades funcionales equivalentes y mantengan la interoperabilidad con el ecosistema.

Asimismo, los endpoints definidos a continuación no constituyen una especificación exhaustiva, sino un conjunto de **referencias comunes** que pueden ser utilizadas para diseñar, validar o comparar soluciones técnicas en distintos contextos.

4.4.1. Endpoints del Servicio de Identidad y Credenciales Verificables

Los siguientes endpoints representan un conjunto de capacidades de referencia que pueden ser consideradas para la emisión, verificación y consulta del estado de credenciales verificables en el espacio de datos.

Su finalidad es facilitar la validación homogénea de identidades en los distintos flujos operativos, pudiendo ser implementados mediante distintas soluciones tecnológicas equivalentes.

Nota interpretativa:

Los niveles indicados (DEBE / DEBERÍA / PUEDE) se interpretan en esta sección como una referencia orientativa de capacidades técnicas dentro del marco de interoperabilidad, y no como obligaciones normativas de implementación para los espacios de datos.

Endpoint	Método	Descripción	Nivel
/credentials/issue	POST	Emisión de credenciales verificables	DEBE
/credentials/verify	POST	Verificación criptográfica de credenciales	DEBE
/credentials/status/{id}	GET	Consulta del estado y revocación	DEBE

Tabla 19. Endpoints del servicio de identidad y credenciales verificables

4.4.2. Endpoints del Registro de Participantes

El Registro de Participantes puede exponer interfaces que permitan consultar el estado, roles y atributos de las entidades dentro del ecosistema.

Estos endpoints facilitan la validación de legitimación y la coherencia del sistema de participación, pudiendo adaptarse a las necesidades específicas de cada implementación.

Endpoint	Método	Descripción	Nivel
/participants	GET	Listado general de participantes activos	DEBERÍA
/participants/{id}	GET	Consulta del estado, roles y atributos de un participante	DEBE
/participants/{id}/history	GET	Historial de cambios (opcional)	PUEDE

Tabla 20. Endpoints del registro de participantes

4.4.3. Endpoints del Catálogo de Recursos

El Catálogo puede ofrecer interfaces abiertas para la publicación, consulta y validación de activos mediante metadatos estructurados.

Estos endpoints permiten habilitar los procesos de descubrimiento e intercambio de forma homogénea, manteniendo flexibilidad en su implementación.

Endpoint	Método	Descripción	Nivel
/catalog/resources	GET	Descubrimiento de activos con filtros	DEBE
/catalog/resources	POST	Publicación de un recurso (metadatos, políticas, calidad)	DEBE
/catalog/resources/{id}	GET	Consulta de ficha completa del activo	DEBE
/catalog/resources/{id}/validate	POST	Validación estructural y semántica	DEBERÍA

Tabla 21. Endpoints del catálogo de recursos

4.4.4. Endpoints de la Biblioteca de vocabularios

La Biblioteca de vocabularios puede proporcionar interfaces para la consulta, gestión y validación de recursos semánticos utilizados en el ecosistema.

Estas capacidades permiten garantizar coherencia semántica entre implementaciones.

Endpoint	Método	Descripción	Nivel
/vocabularies	GET	Listado de vocabularios disponibles	DEBE
/vocabularies/{id}	GET	Consulta de vocabulario y versión	DEBE
/vocabularies/validate	POST	Validación semántica de metadatos	DEBERÍA

Tabla 22. Endpoints de la biblioteca de vocabularios

4.4.5. Endpoints del Motor de Políticas y Contratos

El Motor de Políticas puede ofrecer capacidades para evaluar condiciones de acceso y formalizar acuerdos entre participantes.

Estos endpoints permiten la aplicación automatizada de políticas y la generación de contratos técnicos interoperables.

Endpoint	Método	Descripción	Nivel
/policies/evaluate	POST	Evaluación automática de políticas para negociación o acceso	DEBE
/contracts	POST	Creación del contrato técnico resultante	DEBERÍA
/contracts/{id}	GET	Consulta del contrato asociado a un flujo	DEB

Tabla 23. Endpoints del motor de políticas y contratos

4.4.6. Endpoints del Conector del Espacio de Datos

El conector puede exponer interfaces para iniciar procesos de negociación y transferencia de datos, actuando como punto de interacción entre participantes.

Estas capacidades permiten garantizar interoperabilidad entre soluciones heterogéneas sin imponer una implementación específica.

Endpoint	Método	Descripción	Nivel
/negotiation/initiate	POST	Solicitud inicial de negociación sobre un activo	DEBE
/negotiation/{id}/status	GET	Estado del proceso de negociación	DEBERÍA
/transfer/initiate	POST	Solicitud de transferencia asociada a contrato válido	DEBE
/transfer/{id}/status	GET	Estado de la transferencia	DEBERÍA

Tabla 24. Endpoints del conector del espacio de datos

4.4.1. Endpoints del Servicio de observabilidad

El módulo de observabilidad puede ofrecer capacidades para registrar y consultar evidencias técnicas asociadas a los flujos del espacio de datos.

Estos endpoints permiten la trazabilidad y la verificación del comportamiento del sistema.

Endpoint	Método	Descripción	Nivel
/events	POST	Registro de eventos críticos del flujo (negociación, autorización, transferencia, cierre)	DEBE
/events/{flowId}	GET	Consulta de evidencias asociadas a una operación	DEBE
/events/search	POST	Consulta avanzada de evidencias para auditoría	PUEDE

Tabla 25. Endpoints del servicio de observabilidad

5. Anexo A. Glosario de términos

Acceso

Acción de solicitar u obtener un activo de datos bajo las condiciones definidas en el contrato técnico y evaluadas por el motor de políticas.

Adhesión

Proceso mediante el cual una organización obtiene la condición de participante autorizado del espacio de datos, tras la validación de su identidad y legitimidad y la asignación de roles y atributos.

Activo (o **Producto**)

Agrupación de uno o varios recursos (por ejemplo, una oferta de datos con varias distribuciones, o un servicio con varios *endpoints*).

Atributo

Información verificable asociada a un participante o componente técnico que se utiliza para evaluar políticas, permisos y restricciones dentro del espacio de datos.

Auditoría Técnica

Conjunto de procedimientos destinados a verificar el comportamiento de los componentes del espacio de datos mediante la revisión de evidencias registradas en el sistema de observabilidad.

Biblioteca de Vocabularios

Repositorio en el que se almacenan vocabularios, taxonomías, ontologías y esquemas semánticos utilizados para describir datos y metadatos en el espacio de datos.

Catálogo de Recursos

Componente encargado de almacenar las descripciones estructuradas de los activos de datos y servicios, utilizando un perfil DCAT-AP adaptado al ecosistema.

Conector

Componente técnico que ejecuta las interacciones entre participantes, incluyendo autenticación mutua, negociación, transferencia de datos y registro de evidencias.

Contrato Técnico

Representación legible por máquina del acuerdo alcanzado entre proveedor y consumidor tras la negociación, que define las condiciones de acceso y uso del recurso.

Credencial verificable

Documento digital firmado criptográficamente que certifica la identidad, los atributos o las legitimaciones de un participante o de un componente técnico.

DCAT-AP

Perfil de aplicación europeo de DCAT para describir conjuntos de datos, utilizado como base para los metadatos del Catálogo de Recursos.

Dato

Contenido/*payload* intercambiado o procesado (no alojado en el Catálogo de recursos).

Espacio de Datos

Ecosistema colaborativo que proporciona un medio para que diversos participantes compartan, utilicen datos y presten servicios de manera segura, confiable y conforme a las normativas, con el fin de impulsar la innovación, el impacto económico y social. Basado en un marco de gobernanza, los espacios de datos pueden facilitar transacciones de datos seguras, fomentar la confianza y la soberanía. Estos espacios se pueden implementar mediante arquitecturas interoperables, tecnologías semánticas, conectores y tecnologías de identidad digital, y están diseñados para apoyar una amplia variedad de casos de uso y aplicaciones.

Evaluación de Políticas

Proceso de interpretación automática de permisos, prohibiciones y obligaciones para determinar si un participante puede acceder o utilizar un recurso.

Evidencia Técnica

Registro verificable de una acción o decisión producida durante un flujo operativo, utilizado para trazabilidad, auditoría o certificación.

Flujos Mínimos de Interoperabilidad

Procesos esenciales que permiten operar un espacio de datos: adhesión, publicación, descubrimiento, negociación, transferencia y cierre.

Gobernanza Técnica

Conjunto de mecanismos y servicios que permiten aplicar y supervisar automáticamente las reglas del espacio de datos durante las interacciones técnicas.

Identidad Verificable

Representación digital única de un participante o componente, respaldada por credenciales criptográficas que permiten su validación automática.

Interoperabilidad

Capacidad de que las organizaciones interactúen con vistas a alcanzar objetivos comunes que sean mutuamente beneficiosos y que hayan sido acordados previa y conjuntamente, recurriendo a la puesta en común de información y conocimientos entre las organizaciones, a través de los procesos empresariales a los que apoyan, mediante el intercambio de datos entre sus sistemas de TIC respectivos

Interoperabilidad entre ED

Capacidad de dos espacios de datos distintos para descubrir activos, validar identidades, negociar acuerdos y transferir datos de forma federada.

Motor de Políticas

Componente encargado de interpretar y evaluar políticas legibles por máquina durante la negociación y la transferencia de datos.

Negociación

Proceso mediante el cual proveedor y consumidor acuerdan las condiciones de acceso y uso del activo, generando un contrato técnico.

Observabilidad

Capacidad de registrar, monitorear y auditar las operaciones llevadas a cabo en el espacio de datos y en su interacción con otros espacios de datos.

ODRL

Lenguaje para expresar políticas de uso (permisos, prohibiciones y obligaciones) de forma estructurada y legible por máquina.

Participante

Entidad sujeta al sistema de gobierno que interactúa con el espacio de datos en calidad de productor, proveedor o consumidor de productos de datos y servicios u otro rol.

Política

Regla expresada de forma legible por máquina que determina cómo puede usarse un activo, en qué condiciones y con qué restricciones.

Proceso E2E (Extremo a Extremo)

Secuencia completa de pasos que ejecutan los componentes del espacio de datos desde la adhesión hasta el cierre del ciclo de vida del dato.

PROV-O

Ontología del W3C para describir linaje, trazabilidad y procedencia de datos.

Proveedor de producto de datos

Rol participante del espacio de datos que ofrece productos de datos en el espacio de datos. Los cuales pueden haber sido producidos por él mismo o por otra entidad productora de datos.

Proveedor de servicios

Rol participante que ofrece datos y/o servicios en un espacio de datos. En el caso de que los datos ofertados por el proveedor son generados o producidos por él, tomaría también el rol de productor de datos.

Publicación

Acción de registrar un activo en el Catálogo con sus metadatos, políticas, calidad, linaje y versionado.

Registro de Participantes

Componente que mantiene información verificada sobre identidades, roles, atributos y estado operativo de los participantes.

Recurso

Elemento (*dataset*, API, servicio), descrito en el Catálogo y gobernado por políticas de acceso y uso.

Servicio Habilitador

Componente técnico del espacio de datos (identidad, registro, catálogo, políticas, observabilidad) que proporciona capacidades comunes necesarias para la interoperabilidad.

SHACL

Lenguaje para validar datos RDF, utilizado para comprobar que los metadatos cumplen el perfil semántico del ecosistema.

Soberanía del Dato

Principio por el cual el proveedor conserva control técnico y normativo sobre el acceso, uso, persistencia y destino de sus datos en todo el ciclo de vida.

Transferencia

Flujo mediante el cual el proveedor entrega un dato al consumidor aplicando el contrato técnico y las políticas vigentes.

UNE 0087:2025

Norma española que define los principios, requisitos y orientaciones para la creación y desarrollo de espacios de datos, centrada en interoperabilidad, soberanía y confianza.

6. Anexo B. Gobernanza técnica de la interoperabilidad

La gobernanza técnica de la interoperabilidad constituye el mecanismo que garantiza que un espacio de datos funciona como un ecosistema confiable y verificable, en el que todas las decisiones contractuales, organizativas y normativas se traducen en elementos técnicos que controlan el acceso, el uso y la circulación de los datos. A diferencia de los sistemas centralizados, donde la confianza se deposita en una plataforma, los espacios de datos requieren que la confianza se construya mediante reglas explícitas, mecanismos de control automático y evidencias técnicas verificables en cada interacción entre participantes.

Según la UNE 0087:2025, la gobernanza técnica debe asegurar una aplicación coherente del modelo de gobernanza del espacio de datos, garantizando que todos los componentes (identidad, credenciales, políticas, conectores, catálogo, observabilidad e infraestructura) actúen de forma alineada.

Esta gobernanza técnica implica:

- Mecanismos de identificación y autorización basados en atributos certificados.
- Políticas expresadas en formatos estructurados, legibles por máquina y aplicadas automáticamente.
- Certificación y homologación de participantes, conectores y servicios.
- Segregación de responsabilidades y verificación independiente.
- Un marco de confianza capaz de garantizar integridad, autenticidad y no repudio.
- Sistemas de trazabilidad, auditoría y linaje, imprescindibles para evaluar el cumplimiento.
- Procesos normalizados para incidencias, disputas y sanciones.
- Procedimientos continuos de actualización y adaptación del espacio de datos.

6.1. Roles y responsabilidades

La UNE 0087:2025 establece que los espacios de datos deben definir un modelo claro de roles y responsabilidades que garantice la coherencia entre el diseño de la gobernanza y su materialización técnica. En un ecosistema distribuido la confianza no se deposita en una plataforma única, sino en reglas claras, en atributos verificables y en mecanismos técnicos de control que dependen directamente de los actores implicados.

Gobernar un espacio de datos implica regular a los participantes, los activos y la infraestructura de manera que todos actúen conforme a las políticas generales, los contratos y las obligaciones del modelo de gobernanza. Esta visión implica que los roles no pueden ser ambiguos, deben estar formalmente definidos, tecnológicamente representados (vía credenciales verificables, atributos y permisos) y asociados a procesos verificables de adhesión, operación y supervisión.

El presente apartado define los roles esenciales en la gobernanza técnica de la interoperabilidad, sus responsabilidades y su relación con los mecanismos técnicos descritos en el capítulo anterior.

6.2. Autoridad de gobierno

Responsable de garantizar que el espacio de datos funciona conforme al marco normativo, organizativo y técnico. Su función es asegurar que la interoperabilidad no dependa de decisiones ad-hoc ni de implementaciones tecnológicas aisladas, sino de un conjunto de normas técnicas comunes, auditables y evolutivas.

Según la UNE 0087:2025, este rol es el responsable de desarrollar, mantener, operar y hacer cumplir el modelo de gobernanza del espacio de datos.

Responsabilidades principales:

a) Custodia del marco de confianza.

La autoridad actúa como entidad raíz de confianza del espacio de datos. Esto implica definir los principios del modelo de confianza, registrar las autoridades emisoras de credenciales, mantener las listas de confianza, supervisar la integridad del sistema de identidades, garantizar la validez y renovación de credenciales verificables.

b) Definición y mantenimiento del régimen de políticas técnicas.

Incluye las políticas generales aplicables a todos los actores, las políticas técnicas sobre conectores y servicios, los requisitos mínimos de interoperabilidad, las restricciones de uso vinculadas al dominio del dato y las reglas de seguridad, auditorías y control

c) Supervisión de la conformidad técnica.

La autoridad debe verificar que los componentes cumplen los requisitos de interoperabilidad, supervisar las implementaciones del conector, validar la ejecución de políticas y contratos y revisar los mecanismos de trazabilidad y observabilidad.

d) Decisiones de gobernanza técnica.

Incluye resolver disputas técnicas, interpretar las reglas cuando se producen ambigüedades, activar medidas de excepción o emergencia y coordinar cambios evolutivos en estándares o modelos.

e) Auditoría continua.

La autoridad debe supervisar periódicamente la integridad del registro, la validez de las credenciales, el correcto funcionamiento de conectores, los informes de observabilidad y la calidad de los metadatos y políticas.

f) Rol sancionador.

La especificación UNE 0087:2025 exige capacidad de intervención. La autoridad puede suspender participantes, revocar credenciales, bloquear conectores o limitar operaciones cuando existan incumplimientos.

6.2.1. Operador del Espacio de Datos

El operador técnico es responsable de la operación diaria, estable, segura y eficiente de los servicios técnicos que habilitan el espacio de datos. El operador debe garantizar la continuidad digital del espacio y asegurar el buen funcionamiento del espacio de datos, coordinar la parte operativa y técnica del ecosistema.

Responsabilidades principales:

a) Gestión operativa de los servicios habilitadores.

Incluye catálogo, registro, observabilidad, motor de políticas, cartera digital, API Gateway si procede.

Debe asegurar disponibilidad, escalabilidad, seguridad y resiliencia.

b) Gestión del conector de referencia.

En muchos espacios, la autoridad proporciona un conector de referencia cuya operación y actualización recae sobre el operador técnico.

c) Supervisión de incidentes técnicos.

Debe monitorizar fallos en políticas, errores de validación, problemas de identidad, transacciones fallidas y anomalías de seguridad.

d) Aplicación de medidas correctoras.

En coordinación con la autoridad técnica bloquea flujos incorrectos, aplica políticas de mitigación, corrige configuraciones erróneas y despliega parches.

e) Mantenimiento de la infraestructura.

Incluye actualizaciones, parches de seguridad, copias de respaldo, pruebas de carga y continuidad y supervisión de recursos.

f) Soporte técnico a los participantes.

Ayuda a integrar conectores, publicar datos, diagnosticar errores y validar contratos.

6.2.2. Proveedor de datos o servicios

El proveedor es el rol que ofrece productos de datos en el espacio de datos, los cuales pueden haber sido producidos por él mismo o por otra entidad productora de datos. Debe conservar en todo momento control sobre el destino del dato y las condiciones bajo las que puede ser usado.

Responsabilidades principales:

a) Determinación de políticas de acceso y uso.

El proveedor decide políticas de uso, restricciones contractuales, condiciones de licenciamiento, duración del uso, obligaciones del consumidor.

b) Publicación estructurada en el catálogo.

Debe proporcionar metadatos DCAT-AP, políticas ODRL, condiciones contractuales, descripciones de calidad, información sobre licencias y endpoints para distribución.

c) Gestión del ciclo de vida del dato.

Incluye creación, mantenimiento, retirada y destrucción o archivado.

d) Respuesta durante la negociación.

Debe evaluar ofertas del consumidor, ajustar políticas o rechazar solicitudes.

e) Protección de los activos.

Es responsable de asegurar la calidad, mantener actualizaciones y proteger contra accesos indebidos.

6.2.3. Consumidor

El consumidor utiliza os datos y/o servicios que son ofertados en el espacio de datos. Este rol puede ser asumido tanto por una entidad jurídica como por un usuario vinculado a una organización.

Responsabilidades principales:

a) Cumplir políticas y contratos

Debe ajustar estrictamente a los permisos y prohibiciones del proveedor (ODRL).

b) Solicitar acceso y negociar

Puede solicitar contratos, proponer modificaciones y acordar condiciones alternativas.

c) Garantizar el uso legítimo.

Debe demostrar que solo accede a lo permitido, que respeta duración, finalidad y restricciones y debe informar de incidencias y violaciones.

d) Cooperar en auditorías.

Si existen dudas de cumplimiento, debe facilitar trazas o evidencia interna.

6.2.4. Intermediarios técnicos

Aunque no siempre existe, los intermediarios posibles pueden ser operadores de servicios semánticos, servicios de transformación o actores que operan herramientas de confianza.

Responsabilidades principales:

Ejecutar servicios de valor añadido, garantizar interoperabilidad técnica, operar funciones delegadas bajo supervisión, no acceder a datos sin base contractual y cumplir obligaciones de seguridad y trazabilidad.

6.3. Funciones técnicas del modelo de gobernanza

La gobernanza técnica de un espacio de datos no se limita a la definición de roles o a la existencia de componentes tecnológicos. Debe incluir un conjunto articulado de funciones operativas capaces de traducir las reglas de gobernanza en mecanismo s verificables, automatizados y auditables.

La UNE 0087:2025 exige que estos mecanismos garanticen la coherencia técnica, la integridad del ecosistema, la aplicación de políticas y la protección de la soberanía del dato en todo el ciclo de vida. Por lo tanto, estas funciones son el conjunto de instrumentos necesarios para regular a los participantes, los activos y los recursos tecnológicos. Y sólo mediante estos instrumentos es posible ejercer soberanía digital de forma cierta y verificable.

6.3.1. Gestión del marco de confianza técnico

El marco de confianza es el pilar sobre el que se sostiene la interoperabilidad. Su misión es permitir que los participantes, conectores y servicios del espacio de datos puedan reconocerse entre sí, verificar sus atributos, validar sus autorizaciones y establecer relaciones confiables, sin depender de intermediarios centralizados.

Las funciones clave del marco de confianza son:

a) **Gestión de identidades técnicas y organizativas.** Incluye la identificación inequívoca de participantes, usuarios autorizados, conectores y servicios habilitadores.

Cada identidad debe estar asociada a atributos verificables y a un rol técnico reconocido en el espacio de datos.

b) **Gestión del ciclo de vida de credenciales verificables.**

Debe abarcar emisión inicial tras la validación, actualización de atributos, renovación por incumplimiento o expiración, validación en tiempo real y verificación cruzada entre conectores.

Estas credenciales garantizan que cada entidad actúa según lo permitido.

c) **Mantenimiento de anclas de confianza y registros confiables.**

Incluye lista de participantes confiables, registro de emisores autorizados, registros de políticas generalistas y mecanismos de integridad criptográfica.

d) **Validación continua.**

Se debe verificar que las credenciales no están revocadas, que las identidades son auténticas, que los conectores presentan atributos válidos, que las autorizaciones siguen vigentes y que las políticas siguen aplicándose.

Esto asegura que las relaciones de confianza no son estáticas, sino dinámicas y renovadas continuamente.

6.3.2. Gestión del Registro de Participantes

El Registro de Participantes es el repositorio estructural que mantiene la lógica del ecosistema. Su función no es meramente administrativa, es el punto de referencia técnico para las operaciones de autenticación, autorización, negociación y transferencia.

La UNE0087:2025 establece que este registro debe permitir trazabilidad completa, control sobre el ciclo de vida del participante y aplicación automática de políticas de participación.

Las funciones de registro incluyen:

a) Alta, baja y modificación de participantes.

Cada operación debe estar validada documentalmente, técnicamente y conforme a las reglas del Libro de Reglas.

b) Gestión de roles técnicos.

El registro relaciona:

Identidad → Rol → Credencial → Políticas aplicables

Debe existir un proceso explícito de homologación basado en requisitos técnicos y organizativos.

c) Administración de atributos y legitimaciones.

Los atributos incluyen permisos, capacidades técnicas, roles ampliados y certificaciones adicionales. Estos atributos permiten modelos robustos.

d) Integración con credenciales verificables.

Toda información del registro debe ser verificable, legible por máquina, exportable y consultable por conectores.

e) Relación con listas de confianza y resoluciones.

Incluye suspensiones, revocaciones, sanciones e historial de incidentes.

6.3.3. Gestión del régimen de políticas técnicas

La UNE 0087:2025 atribuye a la gobernanza técnica la responsabilidad de asegurar que las políticas del espacio de datos se aplican de forma consistente, verificable y automatizada.

Las funciones técnicas clave son:

a) Definición y adopción de políticas generales de uso.

Las políticas globales regulan el comportamiento mínimo aceptable, las restricciones comunes, las obligaciones éticas y la seguridad transversal.

b) Transformación de políticas en reglas técnicas.

Incluye la creación de ODRL para permisos, prohibiciones y obligaciones, las reglas formales para XACML y términos técnicos legibles por el conector.

c) Mantenimiento del motor de políticas

El motor debe permitir evaluación dinámica, comprobaciones previas a transferencia, validación continua y coherencia entre contrato y ejecución.

d) Auditoría de políticas aplicadas.

El sistema debe ser capaz de demostrar cuándo se aplicó una política, qué decisión se generó y qué evidencia respalda esa decisión.

6.3.4. Supervisión del ciclo de vida técnico del espacio de datos

Este conjunto de funciones garantiza que el espacio puede evolucionar sin comprometer la interoperabilidad ni la confianza. Se debe garantizar continuidad, mejora continua y capacidad de adaptación. El marco de gobernanza debe adaptarse a medida que el espacio de datos crece o incorpora nuevas partes interesadas.

Incluye:

a) Gestión de actualizaciones técnicas.

Aplicable a conectores, catálogos, servicios habilitadores, modelos de identidad, vocabularios y artefactos semánticos.

b) Control de versiones y compatibilidad.

Debe garantizar compatibilidad con versiones previas, procesos de transición organizados, pruebas antes de migraciones y documentación del impacto.

c) Evaluación continua de requisitos técnicos.

Incluye análisis de cambios normativos, nuevas prioridades del dominio, riesgos emergentes y tecnologías obsoletas.

d) Mecanismos de despliegue controlado.

Las actualizaciones deben poder desplegarse por fases, poderse revertir y ser auditables.

e) Garantía de continuidad operativa.

Hay que implementar redundancias, copias de seguridad, planes de contingencia y rutas alternativas para conectores.

6.4. Certificaciones, homologación y conformidad técnica

La certificación, homologación y verificación de la conformidad técnica constituyen un conjunto de procesos esenciales para garantizar que todos los componentes del espacio de datos – participantes, conectores, servicios habilitadores y mecanismos de control – cumplen los requisitos definidos en el modelo de gobernanza y en la UNE 0087:2025.

Según la norma, la interoperabilidad técnica sólo puede asegurarse si el ecosistema dispone de un mecanismo sistemático que valide la capacidad de cada actor y componente para operar conforme al marco de confianza, las políticas y las obligaciones de seguridad, trazabilidad y soberanía digital.

6.4.1. Objetivos del proceso de certificación técnica

La certificación y homologación tiene como objetivo:

a) **Garantizar interoperabilidad.**

Verificar que participantes, conectores y servicios utilizan estándares, APIs, políticas y mecanismos plenamente conformes con la norma.

b) **Asegurar soberanía digital.**

Confirmar que los conectores implementan correctamente políticas de acceso, restricciones y reglas contractuales, evitando usos indebidos o interacciones fuera del control del proveedor.

c) **Reforzar el marco de confianza.**

Asegurar que identidades, credenciales y atributos cumplen con los requisitos de autenticidad, integridad, revocabilidad y registro establecidos por la autoridad técnica.

d) **Evitar comportamientos no alineados.**

Detectar configuraciones incorrectas, componentes técnicamente inseguros o actores que no cumplan las obligaciones del Libro de Reglas / Libro de Roles.

e) **Garantizar seguridad y trazabilidad.**

Verificar que todos los componentes implementan mecanismos de auditoría, observabilidad y registro según UNE 0087:2025.

6.4.2. Alcance de la certificación y homologación

La certificación técnica debe aplicarse a cuatro elementos:

a) **Participantes.**

Cada organización que se incorpore al ecosistema debe superar un proceso de homologación que valide su identidad, su legitimación jurídica, su rol técnico, sus credenciales verificables y su adecuación a las políticas generales.

b) **Conectores.**

El conector es el componente técnico más crítico y su funcionamiento debe ser verificable. Su certificación incluye validación del plano de control, validación del plano de datos, control de configuración, pruebas funcionales de interoperabilidad y comprobación de cumplimiento del régimen de políticas.

c) **Servicios habilitadores.**

Incluyen el catálogo de recursos, registro de participantes, servicio de credenciales verificables, módulos de observabilidad y motor de políticas. Estos servicios deben cumplir estándares de interoperabilidad, seguridad y control.

d) Políticas, contratos y reglas técnicas.

La certificación técnica también verifica que las políticas están bien definidas y estructuradas, que los contratos son legibles por máquina, que existen mecanismos fiables de valuación y que los conectores pueden ejecutarlos.

6.4.3. Procedimiento general de homologación y certificación

El proceso de certificación costa de varias fases estructuradas:

a) Solicitud y declaración de conformidad.

El participante o componente candidato presenta una solicitud formal, la documentación técnica mínima, la identificación del responsable técnico, la autodescripción técnica del componente y las políticas o servicios que pretende operar.

b) Validación documental.

La Autoridad de gobierno verifica la identidad y legitimación, la coherencia con roles aceptados, políticas que pretende aplicar, cumplimiento preliminar del modelo de confianza, las licencias o requisitos técnicos exigidos.

c) Validación técnica del componente.

Incluye pruebas del plano de control y pruebas del plano de datos.

Las pruebas del plano de control son autenticación mutua, validación de credenciales verificables, evaluación de políticas, negociación conforme a reglas, comunicación con el registro, emisión y validación de tokens. Y las pruebas del plano de datos son la transferencia push/pull, control de cumplimiento contractual, cifrado extremo a extremo, registro de evidencias y manejo de errores y cancelaciones.

d) Emisión de credencial verificable de certificación. Si el componente o participante supera las pruebas se genera una VC de certificación técnica, se inscribe en el Registro de Participantes o en el Registro de Conectores y se actualiza la lista de confianza. Esta credencial habilita la operación técnica en el espacio de datos.

e) Supervisión continua.

La certificación no es un acto puntual, debe existe supervisión continua mediante técnicas de observabilidad, auditorías técnicas periódicas, revisión del cumplimiento y controles ligados a incidentes.

f) Revocación o suspensión.

La Autoridad de gobierno puede revocar certificaciones si se detectan incumplimientos, se compromete el conector, existe mal uso de datos, se incumple la política general y se manipula la infraestructura de forma indebida.

6.4.4. Criterios de conformidad técnica

Para declarar que un componente es conforme, deben verificarse los siguientes criterios alineados con la especificación UNE 0087:2025:

a) Interoperabilidad

Compatibilidad con políticas, APIs, protocolos, estándares y conectores homologados.

b) Seguridad.

Cifrado, integridad, autenticación y autorización robusta.

c) Aplicación de políticas.

El componente debe aplicar restricciones contractuales, obligaciones, permisos y prohibiciones.

d) Trazabilidad

Capacidad de generación de evidencias, logs, eventos, linaje y auditorías exportables.

e) Resiliencia.

Capacidad de gestionar errores, interrupciones y reintentos.

f) Soberanía técnica.

Control de ciclo de uso y de transferencia por parte del proveedor.

6.4.5. Resultados del proceso de certificación

El proceso concluye con uno de tres resultados:

1. **Certificación plena.**

El componente puede operar sin restricciones.

2. **Certificación condicionada.**

Se autoriza con requisitos adicionales a subsanar.

3. **No conforme.**

El componente no puede operar en el espacio de datos.

6.5. Gestión de incidencias y resolución de conflictos

La gestión de incidencias técnicas constituye un mecanismo esencial de la gobernanza técnica del espacio de datos. Según la UNE 0087:2025, la interoperabilidad debe garantizar no solo conectividad y uso conforme a las políticas, sino también la existencia de procedimientos claros para detectar, registrar, analizar, resolver y documentar cualquier desviación técnica o incumplimiento que afecte al funcionamiento del ecosistema.

En un espacio de datos interoperable basado en conectores, políticas legibles por máquina, credenciales verificables y trazabilidad continua, las incidencias técnicas pueden afectar a cualquiera de los elementos del sistema.

La confianza en el ecosistema depende de la capacidad de registrar y analizar cada anomalía, ya que toda acción relevante del ecosistema debe dejar evidencia en el módulo de observabilidad para permitir auditoría y reconstrucción de decisiones. Por tanto, la gestión de incidencias no es reactiva: es preventiva, continua y basada en evidencias.

6.5.1. Tipología de incidencias técnicas.

Para una gestión rigurosa, las incidencias se clasifican en cinco categorías principales:

a) **Incidencias de identidad y credenciales.**

Implica problemas relacionados con validación de identidades, revocación de credenciales, atributos inválidos, discrepancias de roles y credenciales caducadas o mal formadas. Estas incidencias pueden impedir la negociación o transferencia, ya que la identidad es el punto de partida de todo proceso técnico.

b) **Incidencias de políticas y contratos.**

Incluye errores en interpretación de políticas, políticas incompatibles, contratos caducados, conflictos de permisos y prohibiciones, incoherencias entre política y contrato. La evaluación de políticas debe hacerse en cada solicitud de transferencia, de lo contrario puede producirse un uso indebido del dato.

c) **Incidencias de conectividad y transferencia.**

Estas incidencias afectan al plano de datos e incluyen interrupción de flujos push/pull, fallos en cifrado de extremo a extremo, errores de protocolo, timeouts y discrepancias en integridad de la carga útil.

d) **Incidencias en servicios habilitadores.**

Afectan a servicios críticos como catálogo, registro de participantes, motor de políticas, módulo de observabilidad y módulo de identidad. La norma UNE 0087:2025 exige garantizar disponibilidad y resiliencia de estos servicios, por lo que su fallo tiene impacto directo en la interoperabilidad.

e) **Incidencias de incumplimiento.**

Son las más graves, incluyen accesos no autorizados, uso del dato más allá de lo permitido, manipulación de flujos, ocultación de evidencias, alteración de políticas o atributos y modificaciones no autorizadas del conector. Aquí se activa el régimen sancionador técnico.

6.5.2. Mecanismos de detección y alerta

La supervisión debe ser continua, basada en trazabilidad y evidencias. La confianza en los datos pasa por poner a disposición del usuario la historia del linaje del dato, registrar todas las transacciones del ecosistema.

Por tanto, la detección de incidencias debe apoyarse en:

a) **Módulo de observabilidad.**

Recoge cada transacción, cada decisión de política, cada autorización, cada acceso y cada evento relevante del conector. Genera alertas automáticas ante anomalías detectadas.

b) Mecanismos de verificación previa.

Antes de cada negociación o transferencia se verifica la identidad, se valida la credencial, se comprueba la vigencia del contrato y se evalúan políticas. Si algo falla, se genera una incidencia automatizada.

c) Registro de eventos seguros.

Incluye logs estructurados, evidencias de cumplimiento, marcas de tiempo firmadas y reportes de integridad.

d) Monitoreo de conectores.

Incluye fallos de configuración, interrupciones, llamadas incorrectas al registro, errores en tokens y discrepancias entre políticas y ejecución.

6.5.3. Proceso de gestión técnica de incidencias

Todo incidente sigue un flujo claro, normalizado y auditable:

1. **Detección.**

Puede ser automática, iniciada por un componente, reportada por un participante y/o detectada por la autoridad de gobierno.

2. **Registro formal.**

Toda incidencia genera un identificador, una descripción técnica, el componente implicado, la hora exacta, las trazas asociadas y el nivel de severidad. Dicho registro debe ser accesible para análisis posteriores.

3. **Análisis basado en evidencias.**

La autoridad de gobierno o el operador responsable analiza los logs, mensajes de conectores, tokens, metadatos del catálogo, trazas del motor de políticas e historiales de credenciales.

Dicho análisis debe determinar la causa raíz, el impacto técnico, el impacto contractual y el impacto sobre la soberanía del dato.

4. **Decisión técnica.**

La autoridad de gobierno determina la acción apropiada entre las que se encuentran permitir continuidad, reintentar procesos, suspender el flujo, bloquear temporalmente el conector, exigir una revisión, iniciar una revisión, iniciar un proceso de sanción y/o elevar el incidente o gobernanza organizativa.

5. **Aplicación de medidas correctivas.**

Incluyen regeneración de tokens, reaplicación de políticas, actualización de credenciales, reconfiguración de conectores, correcciones en catálogo e intervención en motor de políticas.

6. **Cierre y documentación.**

La incidencia se marca como resuelta y se archiva, documentando el diagnóstico final, las acciones adoptadas, identificando el responsable técnico, enumerando las evidencias generadas y referenciando a políticas o contratos aplicados. Esto garantiza trazabilidad y transparencia.

6.5.4. Resolución de conflictos entre participantes

Cuando una incidencia implica discrepancias entre actores, se exigen procesos claros de resolución. Esto puede ocurrir cuando hay desacuerdo sobre políticas aplicadas, negación de acceso no justificada, denuncia de incumplimiento de contrato y/o errores en la ejecución de políticas por un conector.

El proceso de resolución debe incluir:

a) **Solicitud de aclaración técnica.**

El participante afectado solicita análisis formal.

b) **Revisión técnica por la autoridad.**

Se basa en evidencias del módulo de observabilidad.

c) **Dictamen técnico motivado.**

Incluye interpretación de políticas, análisis del contrato y verificación del comportamiento del conector.

d) **Medidas correctoras o sancionadoras.**

Listado de medidas aplicables según gravedad.

e) **Escalado a la gobernanza organizativa.**

Solo si hay conflicto entre interpretaciones del Libro de reglas o del marco jurídico.

6.5.5. Medidas ante incumplimientos

La autoridad de gobierno puede aplicar las siguientes medidas:

a) **Suspensión temporal de conectores.**

Hasta que se resuelva la incidencia.

b) **Revocación de credenciales verificables.**

En caso de fraude, suplantación o violación grave de políticas.

c) **Limitación de operaciones.**

Restringiendo contratos, accesos o transferencias.

d) **Rechazo automático de solicitudes.**

En función del estado del incidente.

e) **Expulsión técnica del participante.**

En coordinación con gobernanza organizativa.

6.5.6. Integración con auditoría técnica y mejora continua

Toda incidencia debe alimentar el proceso de auditoría, la revisión del marco de políticas, la actualización de conectores, el refuerzo del modelo de confianza y la mejora del motor de políticas.

6.6. Actualización y evolución del marco

La mejora continua y la evolución controlada del modelo técnico constituyen elementos esenciales de la gobernanza de un espacio de datos. Como ya hemos dicho, la interoperabilidad es un proceso dinámico, sometido a cambios tecnológicos, organizativos y normativos que requieren adaptación progresiva y mecanismos estables para garantizar continuidad, cohesión y coherencia en el ecosistema.

La evolución no es opcional, sino inherente al concepto de espacio de datos, a medida que el ecosistema crece, incorpora nuevos actores o amplía sus casos de uso, el marco de gobernanza debe adaptarse para dar cabida a nuevas necesidades, requisitos, estándares y modelos de operación.

La mejora continua, por tanto, no consiste únicamente en actualizar componentes técnicos, sino en garantizar que el espacio de datos mantiene su soberanía, gobernabilidad, interoperabilidad y seguridad a lo largo del tiempo, incluso en entornos de cambio.

1. **Principios para la evolución del espacio de datos**

La evolución del modelo técnico debe seguir los siguientes principios.

a. Continuidad operativa.

Los cambios en estándares, conectores o servicios habilitadores deben garantizar que el espacio de datos sigue funcionando sin interrupciones relevantes.

b. Compatibilidad hacia atrás.

Cuando sea posible, las nuevas versiones deben garantizar que los conectores y servicios ya certificados puedan seguir operando sin rediseños o interrupciones forzadas.

c. Respeto a la soberanía del dato.

La evolución técnica nunca debe comprometer los mecanismos que permiten a los proveedores ejercer control sobre acceso, uso, transferencia, persistencia o destrucción del dato.

d. Evolución basada en evidencias.

Las necesidades de cambio deben surgir de auditorías, incidencias, métricas del sistema, análisis de riesgos o cambios normativos.

e. Transparencia y trazabilidad.

Cada actualización del ecosistema debe quedar documentada, versionada, firmada digitalmente y trazada en el módulo de observabilidad.

f. No discriminación tecnológica.

La evolución técnica debe mantener la neutralidad, permitiendo el uso de distintas tecnologías siempre que las implementaciones cumplan con el marco técnico.

2. Mecanismos para la mejora continua

La UNE 0087:2025 establece que los espacios de datos deben contar con mecanismos sistemáticos para mejor la interoperabilidad, la gobernanza técnica y la calidad del servicio.

Estos mecanismos se estructuran en cinco ejes:

a. Revisión periódica del marco técnico y de las políticas.

La autoridad de gobierno debe revisar de forma periódica políticas generales, restricciones, mecanismos de autorización, uso de modelos y vocabularios, estándares adoptados y configuración del conector.

b. Auditorías técnicas continuas.

Alineado con la sección de observabilidad, las auditorías deben evaluar cumplimiento de políticas, correcto funcionamiento del conector, trazabilidad y evidencias, riesgos de seguridad, calidad del dato, integridad del catálogo y funcionamiento del motor de políticas.

Los resultados deben alimentar las decisiones de mejora.

c. Evaluación de incidentes y lecciones aprendidas.

Cada incidencia registrada constituye una oportunidad de mejora. Esto implica analizar causas raíz, aplicar mejoras técnicas, ajustar políticas, reforzar procesos, actualiza conectores o reglas y documentar lecciones aprendidas.

d. Supervisión de estándares y requisitos normativos.

Los espacios de datos operan en un entorno regulatorio sujeto a cambios (Data Act, DGA, ENS, etc.). La autoridad de gobernanza debe monitorizar nuevos requisitos, evaluar su impacto, adaptar el modelo, introducir nuevas reglas, políticas o controles y realizar transiciones ordenadas.

e. Incorporación de nuevas funcionalidades o dominios.

La evolución puede incluir incorporación de nuevos sectores, adopción de nuevos casos de uso, integración de servicios semánticos más avanzados, incorporación de procesamiento distribuido, nuevos modelos de identidad y mejoras en la arquitectura de conectores.

3. Procedimiento de actualización controlada.

Toda actualización significativa debe seguir un proceso sistemático:

a. Identificación de la necesidad de cambio.

Basada en auditorias, incidentes, cambios en estándares, evolución tecnológica y nuevos requisitos del dominio.

b. Análisis del impacto en el ecosistema.

Incluye evaluación de conectores, de catálogos, de políticas, de identidades, de componentes de seguridad y del registro de participantes.

c. Diseño técnico de la actualización.

Debe documentarse con especificaciones, requisitos, impacto previsto, plan de pruebas y dependencias.

d. Validación por la autoridad de gobierno.

La autoridad debe revisarlo, autorizarlo, publicarlo como nueva versión del marco y registrar el cambo en trazabilidad.

e. Implementación progresiva.

Incluye plan de despliegue gradual, fases de transición, mecanismo para revertir el cambio y coexistencia temporal de versiones.

f. Certificación post-actualización.

Tras aplicar una actualización se deben verificar componentes afectados, se revisan los conectores y se incrementa la supervisión temporal.

g. Documentación y comunicación.

Toda actualización debe quedar documentada, versionada y comunicada a participantes y operadores.

4. Salvaguarda de la continuidad operativa

La continuidad es un principio transversal. El espacio de datos tiene que seguir funcionando incluso ante actualizaciones, fallos, incidentes graves, cambios normativos y evolución tecnológica. Esto implica redundancias, automatización de backups, recuperación ante desastres, verificación del estado de conectores y monitorización reforzada tras actuaciones.

5. Gobernanza del cambio tecnológico

El cambio debe gobernarse con criterios de neutralidad tecnológica, respeto a la soberanía del dato, participación de los actores, evaluación objetiva del riesgo, consenso técnico, alineación con estándares internacionales y normas nacionales.

7. Anexo C. Supervisión, evaluación y mejora continua

La UNE 0087:2025 establece que un espacio de datos debe disponer de mecanismos sistemáticos de supervisión, evaluación y mejora continua que permitan asegurar que los componentes técnicos, las políticas, los procesos de intercambio y los participantes mantienen, en todo momento, un comportamiento conforme a los requisitos del marco técnico, al modelo de gobernanza y a las obligaciones normativas aplicables.

Este enfoque dinámico resulta imprescindible en un entorno donde participante múltiples actores, donde los componentes evolucionan, donde las políticas se actualizan y donde las condiciones de seguridad, calidad y soberanía deben sostenerse de forma constante. La interoperabilidad, entendía como capacidad efectiva de interacción entre sistemas heterogéneos, no se garantiza solo mediante la certificación inicial, sino a través de una vigilancia continuada que permita detectar desviaciones, anticipar riesgos y adoptar medidas de ajuste cuando sea necesario.

En consecuencia, la supervisión técnica debe apoyarse en tres capacidades fundamentales:

1. La medición sistemática del desempeño y el comportamiento del ecosistema.
2. La auditoría técnica basada en evidencias.
3. La mejora continua, que permite que el marco evolucione sin comprometer su estabilidad.

El presente capítulo describe estas capacidades de manera estructurada, definiendo cómo deben aplicarse los indicadores de interoperabilidad, de qué modo deben ejecutarse las auditorías y verificaciones periódicas, y qué procesos deben activarse para que las lecciones aprendidas, los incidentes y las métricas derivadas de la operación del espacio de datos se traduzcan en ajustes del modelo técnico, del régimen de políticas o de los propios componentes.

7.1. Indicadores de desempeño de interoperabilidad

La evaluación sistemática de desempeño técnico del espacio de datos requiere disponer de un conjunto de indicadores que permitan medir, de forma objetiva y verificable, el grado de interoperabilidad alcanzado y el comportamiento efectivo de los componentes que lo integran. De acuerdo con UNE 0087:2025, estos indicadores deben reflejar no solo la capacidad de los participantes para intercambiar datos, sino también la correcta aplicación de políticas, la calidad de las evidencias generadas, la coherencia del ciclo de vida del dato y la resiliencia del ecosistema ante incidencias técnicas o evolutivas.

Por tanto, los indicadores de interoperabilidad no se limitan a parámetros tecnológicos tradicionales (latencia, disponibilidad, respuestas correctas), sino que incorporan dimensiones de gobernanza técnica (validez de identidades, correcta aplicación de

políticas, fiabilidad del conector, coherencia del catálogo, integridad del linaje y consistencia del modelo de confianza).

A continuación, se describen los grandes ámbitos que deben cubrir los indicadores de desempeño:

- **Eficacia de los mecanismos de identidad, atributos y credenciales verificables.**

El modelo de confianza requiere evaluar si el sistema es capaz de identificar correctamente a participantes y componentes, verificar credenciales en tiempo real y garantiza que las autorizaciones se aplican sin ambigüedades.

Indicadores típicos incluyen:

- Proporción de solicitudes rechazadas por credenciales inválidas o caducadas.
- Tiempo medio de validación de credenciales.
- Coherencia entre atributos declarados y atributos utilizados en políticas.
- Incidencias relacionadas con emisiones o revocaciones incorrectas.

Cuando estos indicadores muestran inconsistencias, la soberanía del dato puede verse comprometida.

- **Aplicación efectiva del régimen de políticas.**

La correcta evaluación de políticas por parte de conectores y motores de políticas es uno de los pilares técnicos del ecosistema. Las políticas deben ser interpretadas de la misma manera por todos los componentes.

Los indicadores deben permitir evaluar:

- Si las decisiones de política producidas por distintos conectores son homogéneas para una misma regla.
- Porcentaje de transacciones que activan permisos u obligaciones.
- Frecuencia de conflictos entre políticas detectadas en evaluaciones previas.
- Coherencia entre la política declarada en el catálogo y la aplicada en ejecución.
- Número de transferencias bloqueadas por incumplimiento de política.
- **Desempeño del conector en negociación y transferencia.**

El conector es el ejecutor de la soberanía. La supervisión en su comportamiento requiere indicadores que midan:

- Éxito o fallo en negociaciones contractuales.
- Tiempo de establecimiento de un contrato.
- Latencia y estabilidad de los flujos push/pull.
- Ratio de transferencias abortadas o suspendidas.
- Calidad de la evidencia generada durante la transferencia.
- Cumplimiento de las restricciones de uso en tiempo real.

Estos indicadores permiten verificar que el conector implementa todas las garantías exigidas por el marco técnico.

- **Calidad de los metadatos y activos publicados.**

El catálogo no es solo un repositorio de metadatos, sino un componente de interoperabilidad. La calidad de los activos y sus recursos asociados afecta a la capacidad del ecosistema para descubrir, evaluar y reutilizar datos.

Los indicadores deben reflejar:

- Completitud de perfiles DCAT-AP.
- Coherencia de vocabularios con la Biblioteca de Vocabularios.
- Validez de las políticas asociadas.
- Calidad FAIR/SHACL de los activos.
- Existencia de linaje suficiente para reconstruir el ciclo de vida.
- Número de incidencias vinculadas a datos faltantes o mal descritos.

Si estos indicadores muestran degradación, el espacio de datos pierde valor para sus participantes.

- **Trazabilidad, observabilidad y calidad de evidencias.**

La trazabilidad es un elemento constitutivo del marco técnico. La capacidad de reconstruir totalmente el comportamiento de un conector es condición necesaria para la confianza y para cualquier auditoría.

Los indicadores deben incluir:

- Volumen, coherencia y formato de los eventos generados.
- Porcentaje de operaciones sin evidencia completa.
- Integridad del linaje técnico.
- Capacidad de correlación entre eventos, políticas y contratos.
- Disponibilidad del módulo de observabilidad.

Aquí, un incumplimiento no solo es un fallo técnico, sino un fallo en la gobernanza del espacio de datos.

- **Disponibilidad, resiliencia y estabilidad operativa.**

La interoperabilidad depende también de la salud de los servicios habilitadores y de la infraestructura.

Los indicadores clave incluyen:

- Disponibilidad del catálogo, del registro, del motor de políticas y del módulo de identidad.
- Tiempos de recuperación ante fallos.
- Resistencia a picos de carga.
- Número y tipo de incidentes operativos.
- Latencia de respuesta d ellos servicios esenciales.

Estos indicadores vinculan la interoperabilidad con la continuidad de negocio del ecosistema.

- Cumplimiento de contratos y uso legítimo del dato.

Dado que el espacio de datos ejecuta contratos legibles por máquina, los indicadores deben reflejar el grado de cumplimiento de estos contratos. Pueden incluir:

- Uso permitido versus uso efectivo.
- Frecuencia de violaciones detectadas por el conector.
- Número de accesos o fuera del horario o condiciones permitidas.
- Identificaciones de intentos de reúso indebido.
- Indicadores de riesgo derivados de comportamiento anómalo.
- Madurez y evolución del ecosistema.

La supervisión técnica también debe medir su propia capacidad de mejora, incluyendo:

- Número de recertificaciones completadas.
- Adopción de nuevas versiones del conector.
- Cobertura de formación técnica en participantes.
- Resolución efectiva de incidencias.
- Reducción de errores tras actualizaciones.

La mejora continua exige medir cómo evoluciona el sistema y cómo responde a cambios.

7.2. Auditorías y verificaciones periódicas

La interoperabilidad solo puede sostenerse en el tiempo si existe un sistema permanente de auditorías y verificaciones periódicas que permita comprobar, con evidencia técnica suficiente, que los participantes, los conectores y los servicios habilitadores operan conforme a los requisitos del marco. La UNE 0087:2025 establece que la supervisión de la interoperabilidad debe apoyarse en procedimientos sistemáticos que garanticen el cumplimiento del régimen de políticas, la integridad del modelo de confianza, la correcta aplicación de contratos y la adecuada trazabilidad de las operaciones realizadas.

Las auditorías y las verificaciones periódicas permiten detectar desviaciones, identificar riesgos emergentes, corregir comportamientos anómalos y ajustar el marco técnico cuando sea necesario. Son, además, el mecanismo que conecta la operación diaria del ecosistema con los procesos de evaluación y mejora continua.

- **Naturaleza y alcance de las auditorías.**

Las auditorías pueden ser internas, realizadas por la autoridad de gobierno del espacio de datos o por el operador técnico, o externos, ejecutadas por entidades independientes con competencias en evaluación de conformidad o por organismos designados en el modelo de gobernanza. Ambas modalidades deben regirse por criterios homogéneos y verificables, asegurando que los resultados son comparables y reproducibles.

El alcance de las auditorías abarca tres áreas principales:

a) Componentes técnicos.

Incluye conectores, servicios habilitadores (registro, catálogo, identidad, políticas, observabilidad) y módulos adicionales.

Se comprueba que operan conforme a las especificaciones técnicas, implementan correctamente políticas y contratos, garantizan seguridad y trazabilidad, mantienen la integridad de la evidencia generada y responden adecuadamente ante incidencias.

b) Procesos de interoperabilidad.

Comprende la verificación de flujos de negociación, validación de credenciales, transferencia push/pull, decisiones del motor de políticas, registros de auditoría y trazabilidad.

c) Participantes.

Incluye la revisión del comportamiento técnico de proveedores, consumidores e intermediarios como por ejemplo cumplimiento de políticas, respeto de permisos y obligaciones, correcto uso del conector, coherencia con su rol y atributos declarados, mantenimiento de credenciales y configuraciones.

- **Principios de una auditoría técnica conforme a la UNE 0087:2025.**

Toda auditoría debe respetar los siguientes principios:

a) Veracidad y verificabilidad. Toda conclusión debe basarse en evidencias generadas por componentes del ecosistema, no en apreciaciones subjetivas.
b) Reproducibilidad. El resultado debe ser obtenible nuevamente a partir de la misma evidencia.
c) No intrusividad. Los procesos de auditoría no deben alterar el comportamiento del ecosistema ni comprometer la seguridad.
d) Trazabilidad. Todos los pasos de la auditoría deben quedar documentados y ser recuperables a posterior.
e) Neutralidad tecnológica. Las auditorías evalúan el cumplimiento del marco, no la tecnología utilizada.
f) Proporcionalidad y ámbito definido. Las auditorías deben centrarse en aspectos críticos para la interoperabilidad y la soberanía.

- **Elementos y evidencias utilizados en la auditoría.**

El ecosistema debe proporcionar una colección amplia y estructurada de evidencias que permitan al auditor verificar la conformidad técnica. Entre ellas se incluyen: eventos generados por conectores durante negociaciones y transferencias; decisiones de políticas y contratos aplicados; credenciales verificables presentadas y aceptadas; registros de logs con marca de tiempo firmada; trazas de linaje del dato en el catálogo; datos de configuración del conector; informes de observabilidad agregados; resultados de pruebas realizadas en el sandbox.

- **Metodología de verificación periódica.**

La verificación periódica consiste en un proceso recurrente diseñado para asegurar que el ecosistema mantiene niveles adecuados de interoperabilidad, seguridad y confiabilidad. Debe incluir:

a) Inspección del comportamiento del conector. Revisando su cumplimiento de políticas, consistencia en negociaciones, correcta gestión de tokens, aplicación de contratos y rigor en la evidencia generada.
b) Supervisión de servicios habilitadores. Verificando la disponibilidad del registro, catálogo, módulo de identidad, motor de políticas y observabilidad.
c) Validación de identidades y credenciales. Asegurando que no existen credenciales caducadas, mal emitidas o renovadas incorrectamente.
d) Revisión del cumplimiento contractual. Comprobando que los usos observados coinciden con las reglas del contrato y que no se producen ampliaciones no autorizadas del acceso.
e) Análisis de incidentes. Valorando la recurrencia, severidad y resolución de incidentes técnicos o de incumplimiento detectados.
f) Conformidad con actualizaciones del marco. Verificando que los participantes han adoptado versiones obligatorias del conector o de los servicios y que la infraestructura cumple los requisitos vigentes.

- **Resultados de la auditoría y acciones derivas.**

Los resultados deben documentarse en un informe que describa el grado de conformidad del componente o participante, las desviaciones encontradas, la gravedad y causa de dichas desviaciones, las medidas correctivas exigidas, el impacto en el marco de confianza y la necesidad o no de recertificación.

Dependiendo de los resultados, pueden activarse mejoras técnicas en componentes, actualizaciones de políticas, revisión del catálogo o del registro, medidas correctoras inmediatas, sanciones técnicas y suspensión temporal de un conector o participante.

7.3. Mecanismos de mejora continua

La mejora continua constituye el elemento que permite a un espacio de datos evolucionar, adaptarse y reforzar su nivel de interoperabilidad y soberanía digital a lo largo del tiempo. Este enforque reconoce que la interoperabilidad no es estática, se ve afectada por la evolución tecnológica, por la incorporación de nuevos participantes, por la introducción de nuevos casos de uso y por la adopción de estándares emergentes.

Los mecanismos de mejora continua permiten, por tanto, anticipar riesgos, detectar degradaciones en la interoperabilidad, evitar la obsolescencia de componentes críticos y asegurar que la gobernanza técnica permanezca vigente y eficaz ante nuevos desafíos.

A continuación, se detallan los elementos esenciales de este proceso continuo.

a) Aprendizaje basado en evidencias.

El espacio de datos genera una gran cantidad de información operativa a través del módulo de observabilidad, los conectores, el motor de políticas, el catálogo y el registro de participantes. Esta información constituye la base de la mejora continua, ya que permite

detectar patrones de comportamiento, anomalías, deficiencias en políticas, y oportunidades de optimización.

La evidencia debe ser interpretada mediante un análisis detallado que permita transforma patrones operativos en conocimiento accionable para ajustar el marco técnico y fortalecer la soberanía del dato.

La mejora continua se activa cuando las evidencias revelan:

- Desviaciones en la interpretación o ejecución de políticas.
- Problemas recurrentes de calidad o completitud de metadatos.
- Errores frecuentes em procesos de negociación o transferencia.
- Debilidades em la identificación o en la verificación de credenciales.
- Incoherencias entre componentes certificados.
- Problemas de compatibilidad o estabilidad operativa.
- Tendencias de uso que aconsejen ajustes funcionales.

b) Corrección técnica y actualización del ecosistema.

Cuando se detectan desviaciones o áreas de mejora, la autoridad técnica debe activar procedimientos estructurados corrección que permitan actualizar componentes, modificar configuraciones o ajustar políticas. Estas acciones deben realizarse bajo criterios de neutralidad tecnológicas, transparencia y proporcionalidad, respetando el principio de continuidad operativa.

Las actuaciones derivadas de la mejora continua pueden incluir:

- Actualizaciones de versiones del conector de referencia.
- Revisión del perfil DCAT-AP adoptado o de vocabularios utilizados.
- Ajustes en la definición de roles o atributos.
- Modificación de políticas específicas o generales.
- Nuevas reglas para el motor de políticas.
- Mejoras en el registro de participantes.
- Ampliaciones del módulo de observabilidad.
- Cambios en los requisitos de certificación técnica.

c) Revisión periódica del marco técnico.

La mejora continua implica evaluar de manera periódica la vigencia del marco técnico, asegurando que sus especificaciones siguen siendo adecuadas para las necesidades reales del ecosistema y para el cumplimiento de la normativa vigente. Esta revisión debe considerar:

- La experiencia acumulada durante la operación.
- La evolución tecnológica de entorno digital.
- La aparición de nuevos estándares internacionales.
- Los resultados de auditorías y certificaciones.
- Los cambios regulatorios aplicables a los datos.
- La incorporación de nuevos dominios, sectores o participantes.

Es responsabilidad de la autoridad de gobierno determinar cuándo una revisión del marco debe derivar en la publicación de una nueva versión del modelo técnico, una actualización de políticas o la redefinición de ciertos componentes. Estas actualizaciones deben planificarse de forma ordenada, con periodos de transición y mecanismos de compatibilidad que faciliten su adopción gradual.

d) Retroalimentación estructural entre supervisión y mejora.

Los mecanismos descritos en los apartados anteriores – indicadores, auditorías, verificaciones y evidencias – no son procesos aislados. Deben integrarse en un ciclo iterativo de retroalimentación que permita:

- Identificar problemas o debilidades.
- Analizar su impacto técnico, contractual y organizativo.
- Diseñar acciones correctivas o evolutivas.
- Implementarlas en el ecosistema.
- Verificar su efectividad mediante indicadores y auditorías.
- Actualizar el marco si procede.

e) Participación de los agentes en la mejora continua.

Aunque la autoridad de gobierno lidera el proceso, la mejora continua debe ser un esfuerzo colaborativo. Los proveedores aportan observaciones sobre la calidad y las necesidades del catálogo, los consumidores identifican problemas de acceso, interpretación o negociación, los operadores técnicos detectan debilidades en la infraestructura, y los auditores aportan una perspectiva externa sobre la conformidad y la trazabilidad.

f) Publicación y gobernanza de nuevas versiones.

Finalmente, la mejora continua debe culminar en procesos transparentes de gestión de versiones. Cuando se introduce un cambio técnico o normativo, el ecosistema debe:

- Publicar la nueva versión del componente afectado.
- Garantizar la coexistencia temporal entre versiones antiguas y nuevas.
- Establecer plazos razonables de migración.
- Documentas los cambios y su impacto.
- Registrar en el módulo de observabilidad las fechas y condiciones de actualización.

8. Anexo D. Referencias bibliográficas

1. Reglamento 2023/2854 - ES - EUR-Lex [Internet]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32023R2854

2. Reglamento 2022/868 - ES - EUR-Lex [Internet]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R0868

3. Regulation - EU - 2024/903 - EN - EUR-Lex [Internet]. [citado 22 de mayo de 2025]. Disponible en: https://eur-lex.europa.eu/eli/reg/2024/903/oj/eng

4. Centro de Referencia de Espacios de Datos. ESPECIFICACION UNE 0087:2025 Definición y caracterización de los espacios de datos [Internet]. 2025 [citado 17 de julio de 2025]. Disponible en: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0074731

5. The European Interoperability Framework in detail [Internet]. 2025. Disponible en: https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/european-interoperability-framework-detail

6. Comisión Europea. Una Estrategia Europea de Datos (COM/2020/66 final) [Internet]. 2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020DC0066